"SADAR DIGITAL: PANDUAN PRAKTIS MENJAGA DATA & MELAWAN PINJOL ILEGAL"

Di era digital, akses internet memang mempermudah hidup. Tapi di balik kemudahan itu, ancaman kejahatan digital mengintai siapa saja—dari masyarakat kota hingga pelosok desa. Setiap hari, ribuan orang Indonesia menjadi korban penipuan online, pinjaman ilegal (pinjol ilegal), dan pencurian data pribadi yang berujung pada kerugian finansial, teror psikologis, bahkan tragedi yang mengancam nyawa.

Buku saku "Sadar Digital" hadir sebagai panduan praktis untuk melindungi diri dan keluarga dari kejahatan digital yang semakin canggih. Ditulis dengan bahasa sederhana yang mudah dipahami oleh semua kalangan—termasuk masyarakat desa dengan pendidikan SMP—buku ini memberikan bekal pengetahuan yang langsung bisa dipraktikkan dalam kehidupan sehari-hari.

Apa yang akan Anda dapatkan dari buku ini?

✅ Memahami nilai data pribadi dan mengapa penipu sangat menginginkannya
✅ Mengenali modus phishing seperti undangan palsu dan paket COD yang mencuri data HP
✅ Membedakan pinjol legal vs ilegal dengan checklist yang jelas dan mudah
✅ Cara cek legalitas pinjol hanya dalam 3 menit lewat WhatsApp OJK
✅ Strategi menghadapi teror dari debt collector pinjol ilegal
✅ Script percakapan siap pakai untuk merespons penagih yang mengancam
✅ Langkah hukum yang bisa ditempuh jika menjadi korban
✅ Kontak darurat dan kanal pengaduan ke OJK, Kominfo, dan Polisi

Buku ini tidak hanya berisi teori, tetapi dilengkapi dengan studi kasus nyata, simulasi percakapan, checklist keamanan digital, dan panduan visual yang memudahkan pembaca untuk langsung menerapkan ilmunya. Dari remaja hingga orang tua, dari petani hingga pegawai kantor, semua bisa memahami dan mempraktikkan isi buku ini.

Jangan tunggu sampai menjadi korban!
Lindungi diri, keluarga, dan data pribadi Anda mulai hari ini. Karena di dunia digital, pengetahuan adalah pertahanan terbaik.

"Data Pribadi = Harta Karun. Jaga seperti Anda menjaga emas dan perhiasan."

Cekli Setya Pratiwi, SH., LL.M., M.CL., Ph.D.
&
Prof. Dr. Sidik Sunaryo, SH., M.Si., M.Hum.

UMM
www.umm.ac.id

Sadar Digital: Panduan Praktis Menjaga Data & Melawan Pinjol Ilegal

Cekli Setya Pratiwi, SH., LL.M., M.CL., Ph.D.

&

Prof. Dr. Sidik Sunaryo, SH., M.Si., M.Hum.

UMM
UNIVERSITAS MUHAMMADIYAH MALANG

HALAMAN HAK CIPTA

SADAR DIGITAL PANDUAN PRAKTIS MENJAGA DATA & MELAWAN PINJOL ILEGAL

Penulis: Cekli Setya Pratiwi, SH., LL.M., M.CL., Ph.D. Prof. Dr. Sidik Sunaryo, SH., M.Si., M.Hum.
Editor: Tim Editor Akademis
Desainer Sampul: Tim Desain Grafis
Penerbit: JIK-Creative Malang, Indonesia
Cetakan Pertama: Desember 2025
Hak Cipta © 2025 oleh Cekli Setya Pratiwi dan Prof. Dr. Sidik Sunaryo
Hak cipta dilindungi undang-undang. Dilarang memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari penerbit.

ISBN: 978-[XXXXXXXX-X]

DISCLAIMER (SANGKALAN)
Buku ini bertujuan untuk **edukasi dan peningkatan literasi digital** masyarakat Indonesia.
Penting untuk diketahui:

1. **Bukan Nasihat Hukum Profesional** - Informasi dalam buku ini adalah panduan umum dan BUKAN pengganti konsultasi hukum profesional.
2. **Konsultasi Diperlukan** - Untuk masalah hukum serius, segera konsultasikan dengan pengacara atau profesional hukum yang berpengalaman.
3. **Perubahan Hukum** - Informasi akurat hingga Desember 2025. Hukum dapat berubah setelahnya.
4. **Kontak Resmi** - Untuk laporan resmi, hubungi lembaga resmi: OJK (157), Kominfo (aduankonten.id), atau Kepolisian (patrolisiber.id).
5. **Tanggung Jawab** - Penulis dan penerbit tidak bertanggung jawab atas kerugian yang timbul dari penggunaan informasi dalam buku ini.

Katalog Dalam Terbitan (KDT)
Pratiwi, Cekli Setya; Sunaryo, Sidik **Sadar Digital: Panduan Praktis Menjaga Data & Melawan Pinjol Ilegal** / Cekli Setya Pratiwi, Sidik Sunaryo. – Malang: JIK-Creative, 2025. 28 hlm.; 15 × 21 cm ISBN 978-[XXXXXXXX-X]
I. Hukum - Keamanan Data II. Pinjaman Online III. Judul
343.099

Cetak di Indonesia | Printed in Indonesia
© JIK-Creative - 2025

KATA PENGANTAR

Assalamu'alaikum warahmatullahi wabarakatuh,

Puji syukur kita panjatkan kepada Allah SWT atas segala rahmat dan karunia-Nya, sehingga buku "Sadar Digital: Panduan Praktis Menjaga Data & Melawan Pinjol Ilegal" ini dapat hadir di tangan pembaca.

Di era digital, lebih dari 215 juta orang Indonesia kini terhubung ke internet. Kemudahan akses informasi dan transaksi keuangan memberikan banyak manfaat, namun di balik itu ancaman kejahatan digital dan pinjol ilegal semakin mengintai masyarakat yang literasi digitalnya masih rendah. Literasi digital bukan sekadar kemampuan teknis menggunakan teknologi, tetapi juga pemahaman tentang keamanan dan perlindungan diri di dunia maya. Tanpa bekal yang memadai, masyarakat rentan menjadi korban phishing, pencurian data, dan teror pinjol ilegal yang dapat menghancurkan kehidupan seseorang dan keluarganya.

Buku ini kami tulis dengan semangat untuk memberikan kontribusi nyata bagi masyarakat Indonesia, khususnya mereka yang tinggal di daerah pedesaan dan memiliki keterbatasan akses terhadap pendidikan keamanan digital. Buku ini ditulis dengan bahasa sederhana, mudah dipahami, dan langsung bisa dipraktikkan dalam kehidupan sehari-hari.

Harapan kami, buku ini dapat menjadi perisai bagi masyarakat dalam menghadapi ancaman kejahatan siber dan jeratan utang ilegal. Kami berharap setiap pembaca tidak hanya memahami risiko yang ada, tetapi juga memiliki pengetahuan praktis untuk mencegah, menghadapi, dan melaporkan kejahatan digital. Lebih dari itu, kami berharap buku ini dapat disebarluaskan ke keluarga, tetangga, dan masyarakat di sekitar Anda, sehingga semakin banyak orang yang terlindungi dari ancaman digital.

Kami menyadari bahwa buku ini tidak sempurna. Kritik dan saran yang membangun sangat kami harapkan untuk perbaikan di masa mendatang. Terima kasih kepada semua pihak yang telah mendukung penerbitan buku ini.

Semoga buku ini memberikan manfaat yang sebesar-besarnya bagi masyarakat Indonesia dan menjadi bagian dari upaya kolektif membangun Indonesia yang lebih sadar digital, aman, dan berdaya.

Wassalamu'alaikum warahmatullahi wabarakatuh.

Malang, Desember 2025
Cekli Setya Pratiwi, SH., LL.M., M.CL., Ph.D.
Prof. Dr. Sidik Sunaryo, SH., M.Si., M.Hum.

HALAMAN HAK CIPTA **1**

KATA PENGANTAR **2**

BAGIAN 2: PENDAHULUAN **4**

Mengapa Buku "Sadar Digital" Ini Penting? 4
Kenapa Anda Perlu "Sadar Digital"? 4
Bahasa yang Gampang Dimengerti 4
Panduan Praktis, Bukan Teori Saja 4
Apa Itu Warga Digital? 5
Bekal Anda di Buku Ini 5

BAGIAN 3: MODUL 1 - JAGA DATAMU, JAGA DIRIMU **6**

Apa Itu Data Pribadi? 6
Jenis Data Pribadi 6
Mengapa Data Kita Berharga? 7
Risiko Nyata KTP dan Foto Selfie 8
Hak-Hak Warga Menurut UU PDP 8
Waspada Phishing (Pencurian Data) 9
Studi Kasus & Simulasi 1 (Modus Undangan/Paket) 10
Bedah Kasus: OTP = Password Rahasia 12
Rangkuman Modul 1 15

BAGIAN 4: MODUL 2 - CERDAS FINANSIAL, LAWAN PINJOL ILEGAL **17**

Pinjol Legal vs Pinjol Ilegal 17
Bahaya "Camilan" (Cepat, Mudah, Ngeri Belakangan) 19
Strategi Jika Terlanjur Terjerat (Bagian 1) 22
Strategi Menghadapi Teror (Bagian 2) 22
Simulasi Role-Playing: Merespon Penagih (Skenario B) 25
Fatwa dan Pandangan Hukum 28
Rangkuman Modul 2 30

BAGIAN 5: PENUTUP & REFERENSI **34**

Checklist Keamanan Digital (Lembar Potong/Copy) 34
Skor Keamanan Digital Anda 36
Kontak Penting & Kanal Pengaduan 38

DAFTAR ISTILAH (GLOSARIUM) **43**

GLOSARIUM ISTILAH KEAMANAN DIGITAL 43
Tips Menggunakan Glosarium Ini 46

DAFTAR PUSTAKA (BIBLIOGRAPHY) **47**

BIOGRAFI PENULIS **53**

Cekli Setya Pratiwi, SH., LL.M., M.CL., Ph.D. 53
Prof. Dr. Sidik Sunaryo, SH., M.Si., M.Hum. 53

BAGIAN 2: PENDAHULUAN

Mengapa Buku "Sadar Digital" Ini Penting?

Indonesia sekarang menjadi salah satu negara dengan pengguna internet terbanyak di Asia Tenggara. Menurut data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), lebih dari 215 juta orang atau sekitar 78% penduduk Indonesia sudah bisa mengakses internet pada 2024. Teknologi digital memang mempermudah hidup kita, mulai dari belanja online, transfer uang, sampai mencari informasi dengan cepat. Tapi kemudahan ini juga membuka pintu bagi penjahat digital yang semakin pintar memanfaatkan ketidaktahuan masyarakat.

Kerugian akibat kejahatan digital bukan sekedar angka di koran, tapi kerugian nyata yang dialami jutaan orang. Otoritas Jasa Keuangan (OJK) mencatat bahwa kerugian masyarakat akibat pinjaman online (pinjol) ilegal mencapai triliunan rupiah. Ribuan orang mengadu karena diintimidasi oleh penagih utang, data pribadi mereka disebarkan ke kontak keluarga dan teman, bahkan ada yang sampai bunuh diri karena tidak tahan dipermalukan. Pinjol ilegal mengambil data pribadi kita tanpa izin seperti daftar kontak, foto di galeri, sampai lokasi kita berada, lalu menyebarkannya untuk mempermalukan korban. Belum lagi penipuan investasi bodong, pesan palsu lewat WhatsApp, dan akun media sosial yang diretas untuk minta uang ke teman dan keluarga kita.

Kenapa Anda Perlu "Sadar Digital"?

Melindungi Diri Dimulai dari Pengetahuan Buku "Sadar Digital: Panduan Praktis Menjaga Data & Melawan Pinjol Ilegal" hadir untuk memberi Anda bekal pengetahuan yang langsung bisa dipraktikkan. Dengan memahami cara kerja penipu, hak Anda sebagai korban, dan langkah pencegahan sederhana seperti memeriksa izin aplikasi sebelum memasang atau mengenali ciri situs palsu, risiko menjadi korban bisa diperkecil.

Bahasa yang Gampang Dimengerti

Hukum sering terasa rumit dan jauh dari kehidupan sehari-hari. Buku ini ditulis dengan bahasa sehari-hari seperti ngobrol dengan teman, tapi tetap akurat. Setiap istilah yang mungkin asing dijelaskan dengan contoh sederhana agar siapa pun, dari remaja sampai orang tua, bisa langsung paham dan menerapkannya.

Panduan Praktis, Bukan Teori Saja

Anda akan menemukan daftar periksa keamanan, langkah hukum yang jelas (seperti cara membuat laporan ke Polisi atau mengajukan gugatan), contoh surat laporan, dan kasus nyata yang terjadi di Indonesia. Tidak ada istilah rumit atau pasal undang-undang yang membingungkan tanpa penjelasan. Semuanya disajikan dalam bentuk ringkas dan bisa langsung dilakukan.

💡 Ingat: Kejahatan digital berkembang lebih cepat dari kesadaran masyarakat. Jangan tunggu sampai menjadi korban baru mulai belajar melindungi diri dan data pribadi Anda.

Apa Itu Warga Digital?

Warga digital adalah kita semua yang menggunakan internet dan teknologi dalam kehidupan sehari-hari. Kalau Anda pernah menggunakan handphone untuk WhatsApp, belanja online, transfer uang lewat mobile banking, atau sekedar lihat berita di media sosial, berarti Anda sudah menjadi warga digital. Di dunia maya, kita juga punya hak dan kewajiban sama seperti di dunia nyata. Ada aturan yang harus dipatuhi, ada etika yang harus dijaga, dan ada tanggung jawab yang harus dipenuhi. Di Indonesia, perilaku kita di dunia digital diatur dengan UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) yang melindungi kita sekaligus memberi batasan agar tidak merugikan orang lain.

Bekal Anda di Buku Ini

Buku "Sadar Digital" ini dibagi menjadi beberapa modul yang akan membekali Anda dengan pengetahuan praktis. Modul 1 akan membahas tentang cara menjaga data pribadi Anda agar tidak jatuh ke tangan yang salah, mulai dari mengatur privasi aplikasi sampai mengenali tanda-tanda penipuan. Modul 2 akan fokus pada cara melawan pinjol ilegal, termasuk hak Anda sebagai korban, langkah hukum yang bisa diambil, dan kemana harus melapor. Kedua modul ini adalah bekal utama agar Anda bisa menjadi warga digital yang cerdas, aman, dan tidak gampang ditipu.

BAGIAN 3: MODUL 1 - JAGA DATAMU, JAGA DIRIMU

Apa Itu Data Pribadi?

Data pribadi adalah semua informasi tentang diri kita yang bisa digunakan untuk mengenali kita, baik secara langsung maupun tidak langsung. Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik melalui sistem elektronik (seperti aplikasi di handphone) atau nonelektronik (seperti dokumen kertas). Misalnya, kalau ada orang yang tahu nama lengkap dan tanggal lahir kita, mereka bisa mengenali siapa kita. Kalau data ini digabung dengan informasi lain seperti alamat rumah atau nomor telepon, identitas kita semakin jelas.

UU PDP membagi data pribadi menjadi dua kategori besar, yaitu data pribadi umum dan data pribadi spesifik. Data umum adalah informasi yang sifatnya bisa diketahui orang untuk mengenali kita, seperti nama atau tempat tinggal. Sedangkan data spesifik adalah informasi yang lebih sensitif dan kalau disalahgunakan bisa menimbulkan dampak besar seperti diskriminasi atau kerugian finansial.

Jenis Data Pribadi

Jenis Data	Kategori	Contoh	Mengapa Penting Dilindungi
Data Pribadi Umum	Informasi dasar identitas	Nama lengkap, tempat dan tanggal lahir, jenis kelamin, agama, status perkawinan, alamat rumah, nomor telepon, email	Bisa digunakan untuk mengenali dan menghubungi kita. Kalau jatuh ke tangan penipu, bisa dipakai untuk modus penipuan
Data Pribadi Spesifik	Data kesehatan	Riwayat penyakit, hasil tes laboratorium, rekam medis	Bisa digunakan untuk diskriminasi (misalnya ditolak kerja karena punya penyakit tertentu)
	Data biometrik	Sidik jari, foto wajah, rekaman suara, scan retina mata	Unik untuk setiap orang dan tidak bisa diubah. Kalau dicuri, bisa dipakai untuk membobol keamanan

Jenis Data	Kategori	Contoh	Mengapa Penting Dilindungi
	Data keuangan	Informasi rekening bank, gaji, aset, utang, riwayat transaksi	Bisa digunakan untuk pencurian uang atau penipuan pinjaman atas nama kita
	Data anak	Semua informasi tentang anak di bawah umur	Anak lebih rentan dimanfaatkan. Butuh izin orang tua untuk menggunakan data anak
	Data genetika	Informasi tentang DNA atau keturunan	Sangat sensitif dan bisa dipakai untuk berbagai kepentingan yang merugikan
	Catatan kejahatan	Catatan kriminal atau pelanggaran hukum	Bisa digunakan untuk mempermalukan atau mendiskriminasi seseorang

UU PDP dengan tegas melarang siapa pun untuk mengumpulkan, mengungkapkan, atau menggunakan data pribadi orang lain secara melawan hukum. Kalau ada aplikasi pinjol yang menyebarkan foto dan kontak kita tanpa izin, itu melanggar UU PDP dan bisa dilaporkan.

Mengapa Data Kita Berharga?

Data Seperti Perhiasan dan Emas

Dalam dunia digital, data pribadi kita sama berharganya dengan perhiasan emas atau sertifikat tanah yang kita simpan rapat-rapat. Bayangkan kalau perhiasan emas atau sertifikat tanah warisan kita dicuri, pasti kita akan sangat dirugikan. Data pribadi kita pun begitu. Data pribadi kita sangat berharga bagi pelaku kejahatan karena bisa digunakan untuk penipuan atau akses ilegal ke akun pribadi kita. Penipu bisa menjual data kita ke pihak lain seperti menjual barang curian, menggunakannya untuk membobol rekening bank, atau bahkan meminjam pinjol atas nama kita tanpa sepengetahuan kita. Bayangkan kalau tiba-tiba ada tagihan pinjol jutaan rupiah yang sebenarnya tidak pernah kita pinjam, hanya karena KTP dan data kita sudah dicuri. Atau rekening kita tiba-tiba kosong karena dibobol menggunakan informasi pribadi yang bocor. Itulah sebabnya penipu sangat menginginkan data kita, karena bagi mereka data adalah uang.

Risiko Nyata KTP dan Foto Selfie

KTP dan foto selfie yang tersebar adalah kombinasi berbahaya yang sering dimanfaatkan penipu. Dengan hanya bermodalkan foto KTP dan foto selfie kita, penipu bisa berpura-pura menjadi kita untuk membuka akun pinjol ilegal, mengajukan pinjaman ke bank, bahkan membuat akun palsu untuk menipu orang lain. Mereka bisa menyamar sebagai kita dan melakukan tindakan yang merugikan seperti penipuan keuangan atau membuka akun bank atas nama kita. Kasus yang banyak terjadi adalah seseorang tiba-tiba didatangi debt collector pinjol karena identitasnya dicatut untuk pinjaman yang tidak pernah diajukan. Foto selfie dengan KTP yang biasa diminta saat mendaftar aplikasi ternyata bisa disalahgunakan untuk verifikasi identitas di berbagai layanan keuangan. Bahkan identitas kita bisa dijadikan modus penipuan dengan berpura-pura jadi orang yang dikenal oleh targetnya sehingga korban akan lebih mudah percaya. Karena itu, jangan sembarangan memberikan foto KTP dan foto selfie ke aplikasi atau orang yang tidak jelas.

Hak-Hak Warga Menurut UU PDP

Hak untuk Tahu dan Mendapat Informasi

Sebagai pemilik data pribadi atau subjek data pribadi, kita punya hak yang dilindungi oleh UU Perlindungan Data Pribadi (UU PDP). Hak pertama dan paling penting adalah hak untuk mendapatkan informasi yang jelas tentang penggunaan data kita. Menurut Pasal 5 UU PDP, kita berhak tahu siapa yang meminta data pribadi kita, untuk tujuan apa data kita dipakai, apa dasar hukumnya, dan siapa yang bertanggung jawab kalau terjadi penyalahgunaan. Selain itu, kita juga berhak untuk mengubah dan memperbaiki data pribadi kita agar tetap akurat, berhak mendapatkan salinan data pribadi kita secara gratis, dan berhak untuk menarik kembali persetujuan yang sudah kita berikan sebelumnya. Jadi, kalau ada aplikasi yang meminta data kita tapi tidak mau memberitahu untuk apa data tersebut digunakan, itu melanggar hak kita.

Hak Menghapus Data dan Mengajukan Keberatan

Kita juga punya hak untuk menghapus data pribadi kita yang sering disebut "right to be forgotten" atau hak untuk dilupakan. Menurut Pasal 8 UU PDP, kita berhak untuk mengakhiri pemrosesan, menghapus, atau memusnahkan data pribadi kita sesuai dengan ketentuan peraturan yang berlaku. Misalnya, kalau kita dulu pernah mendaftar di aplikasi pinjol legal tapi sekarang sudah tidak pakai lagi dan tidak punya utang, kita bisa meminta mereka menghapus semua data kita dari sistem mereka. Selain itu, kita juga berhak mengajukan keberatan kalau data kita disalahgunakan, seperti disebarkan tanpa izin atau dipakai untuk keputusan yang merugikan kita. Yang paling penting, kalau terjadi pelanggaran terhadap data pribadi kita, kita berhak untuk menggugat dan menerima ganti rugi sesuai dengan undang-undang. Jadi jangan takut untuk memperjuangkan hak kita kalau data pribadi kita disalahgunakan.

Waspada Phishing (Pencurian Data)

Apa Itu Phishing?

Phishing berasal dari kata "fishing" yang artinya memancing. Disebut memancing karena penipu berusaha memancing kita untuk memberikan informasi pribadi yang sensitif seperti password, PIN, nomor kartu kredit, atau kode OTP. Penipu biasanya menyamar menjadi pihak yang terlihat resmi dan terpercaya seperti petugas bank, kurir paket, atau bahkan teman yang mengirimkan undangan pernikahan. Mereka mengirim pesan lewat WhatsApp, SMS, atau email yang terlihat seperti pesan asli dari perusahaan besar atau lembaga pemerintah. Isi pesannya biasanya mendesak kita untuk segera bertindak, misalnya "Paket Anda tertahan, klik link ini untuk mengambil" atau "Akun bank Anda bermasalah, segera update data". Begitu kita mengklik tautan dan memasukkan informasi pribadi, data kita langsung dicuri dan digunakan untuk kejahatan seperti menguras rekening atau membuat pinjaman atas nama kita.

Bahaya File APK Palsu

Yang paling berbahaya adalah file APK palsu yang dikirim melalui pesan atau link. APK adalah file untuk memasang aplikasi di handphone Android. Penipu sering mengirimkan file APK dengan nama yang menipu seperti "Undangan.apk", "FotoPaket.apk", atau "BonusPulsa.apk". Kalau kita memasang file APK ini di handphone, sebenarnya kita sedang memasang aplikasi jahat yang bisa menyedot semua data di HP kita seperti daftar kontak, foto, pesan WhatsApp, bahkan informasi mobile banking. Aplikasi jahat ini juga bisa membaca kode OTP yang masuk ke SMS kita, sehingga penipu bisa membobol rekening bank tanpa sepengetahuan kita. Ingat, aplikasi resmi tidak pernah dikirim lewat WhatsApp atau SMS, tetapi selalu diunduh dari Google Play Store. Jangan pernah memasang file APK yang dikirim oleh orang yang tidak kita kenal atau bahkan oleh teman, karena bisa saja akun teman kita sudah diretas..

Studi Kasus & Simulasi 1 (Modus Undangan/Paket)

📱 Contoh Pesan Penipuan

Bedah Kasus: Ciri-Ciri Pesan Penipuan

1. Nomor Pengirim Tidak Dikenal atau Asing

Penipu biasanya menggunakan nomor yang tidak ada di kontak kita dan mengirim pesan secara acak tanpa memperkenalkan diri. Kalau ada nomor asing yang tiba-tiba mengirim undangan atau info paket, sudah pasti mencurigakan.

2. Mendesak Korban Mengklik File

Pesan biasanya sangat singkat dan langsung meminta kita untuk membuka file, tanpa penjelasan yang jelas. Penipu tidak mau menjawab pertanyaan seperti "Siapa yang menikah?" atau "Paket dari mana?" karena tujuannya hanya memancing kita mengklik file.

3. File Berekstensi Aneh (APK)

Yang paling berbahaya adalah file dengan nama berakhiran .apk seperti "Undangan Pernikahan Digital.apk", "Resi Paket.apk", "Lembar Tagihan.apk", atau "PLN.apk". File APK adalah aplikasi Android yang kalau dipasang bisa mencuri semua data di HP kita termasuk kode OTP mobile banking. Undangan atau foto asli biasanya berformat JPG, PNG, atau PDF, bukan APK.

4. Ukuran File Mencurigakan

File undangan atau foto biasa ukurannya kecil, tapi file APK penipu biasanya 5-7 MB karena berisi aplikasi jahat.

⚠️ Tips: Apa Yang Harus Dilakukan?

JANGAN:

- Jangan klik atau buka file dengan ekstensi .apk yang dikirim lewat WhatsApp
- Jangan pasang aplikasi dari sumber yang tidak jelas
- Jangan berikan informasi pribadi seperti password, PIN, atau kode OTP kepada siapa pun

LAKUKAN:

- Tanya dulu siapa pengirimnya kalau dapat undangan dari nomor tidak dikenal
- Kalau mencurigakan, langsung blokir nomor tersebut dan hapus pesannya
- Lapor ke kontak resmi bank Anda jika merasa sudah terlanjur mengklik
- Lapor ke kepolisian atau OJK jika menjadi korban
- Ingat, aplikasi resmi hanya diunduh dari Google Play Store, bukan dari WhatsApp

💡 Ingat: Kalau ada yang kirim file .apk lewat WhatsApp, itu 99% penipuan. Undangan asli biasanya berupa gambar atau link ke website undangan, bukan aplikasi.

Studi Kasus & Simulasi 2 (Social Engineering)

📞 Contoh Skenario Penipuan Telepon

☎️ Panggilan Masuk: 021-XXXXXXX

Penipu: "Selamat siang, dengan Bapak Ahmad? Saya dari Divisi Keamanan Bank XYZ. Kami mendeteksi ada transaksi mencurigakan sebesar Rp 5 juta dari rekening Bapak."

Korban: "Wah, saya tidak melakukan transaksi itu!"

Penipu: "Baik Pak, untuk membatalkan transaksi ini, Bapak perlu verifikasi dulu. Nanti akan ada SMS berisi kode OTP, tolong dibacakan ke saya ya Pak agar transaksi bisa dibatalkan."

Korban: "Oh baik... kode OTP-nya 234567."

Penipu: "Terima kasih Pak, transaksi sedang diproses pembatalan..."

[5 menit kemudian, rekening korban terkuras habis]

Bedah Kasus: OTP = Password Rahasia

Apa Itu OTP?

OTP atau One Time Password adalah kode rahasia yang dikirim lewat SMS atau aplikasi untuk memverifikasi bahwa benar kita yang melakukan transaksi. Kode OTP ini hanya berlaku satu kali dan dalam waktu singkat, biasanya 3-5 menit. OTP berfungsi sama seperti password atau PIN ATM kita, jadi sifatnya sangat rahasia.

Mengapa OTP Tidak Boleh Diberikan?

OTP adalah kunci terakhir untuk mengakses rekening atau melakukan transaksi atas nama kita. Kalau kita memberikan kode OTP kepada orang lain, sama saja dengan memberikan kunci brankas kita kepada pencuri. Dengan kode OTP, penipu bisa menguras rekening, mengubah password mobile banking, atau bahkan mengalihkan nomor HP kita ke perangkat mereka.

Fakta Penting yang Harus Diingat:

Petugas bank TIDAK PERNAH dan TIDAK AKAN PERNAH meminta kode OTP, PIN, password, atau nomor CVV/CVC kartu kepada nasabah. Kalau ada yang mengaku petugas bank dan meminta kode OTP, sudah pasti itu penipu. Bank sudah punya sistem sendiri untuk mengecek transaksi nasabah tanpa perlu meminta kode OTP.

🚨 **Ingat Selalu!**

HARAM MEMBERIKAN:

- Kode OTP (One Time Password)
- PIN ATM atau mobile banking
- Password akun bank
- Nomor CVV/CVC (3 angka di belakang kartu)
- m-Token atau kode keamanan lainnya

Kepada siapa pun, termasuk:

- Orang yang mengaku petugas bank
- Customer service
- Polisi atau instansi pemerintah
- Teman atau keluarga yang meminjam HP kita

💡 Ingat: Kode OTP adalah kunci pribadi Anda. Bank tidak akan pernah meminta OTP lewat telepon, email, WhatsApp, atau SMS. Kalau ada yang minta, langsung tutup telepon dan lapor ke bank.

Tips Aman Bermedia Sosial

Media sosial seperti Facebook, Instagram, WhatsApp, dan TikTok sudah menjadi bagian dari kehidupan sehari-hari. Namun, kalau tidak hati-hati, media sosial bisa menjadi pintu masuk bagi penipu untuk mencuri data pribadi kita. Berikut adalah checklist keamanan yang harus Anda terapkan untuk melindungi diri dan keluarga di dunia digital.

✅ **Checklist Keamanan Media Sosial**

No.	Yang Harus Dilakukan	Mengapa Penting?	Status
1	**Jangan posting foto KTP, SIM, atau dokumen identitas**	Foto KTP bisa digunakan penipu untuk membuka pinjol ilegal atau membuat akun palsu atas nama kita	☐
2	**Jangan posting tiket pesawat (boarding pass)**	Boarding pass berisi kode booking yang bisa digunakan untuk mengakses data perjalanan kita dan membatalkan tiket	☐
3	**Sembunyikan tanggal lahir lengkap**	Tanggal lahir sering digunakan sebagai password atau pertanyaan keamanan. Penipu bisa memanfaatkannya untuk meretas akun	☐
4	**Sembunyikan alamat rumah lengkap**	Alamat bisa digunakan penipu untuk modus pengiriman paket palsu atau kejahatan fisik lainnya	☐
5	**Batasi visibilitas nomor telepon**	Nomor telepon bisa digunakan untuk modus penipuan via WhatsApp atau SMS phishing	☐
6	**Atur privasi akun menjadi "Pribadi" atau "Teman Saja"**	Agar tidak semua orang bisa melihat foto, postingan, dan informasi pribadi kita	☐
7	**Jangan sembarangan terima permintaan pertemanan dari orang asing**	Akun palsu sering digunakan untuk mengintai informasi kita atau menyebarkan penipuan	☐
8	**Ganti password secara berkala (minimal 3 bulan sekali)**	Password lama bisa bocor tanpa kita sadari. Ganti password secara berkala memperkecil risiko akun diretas	☐

No.	Yang Harus Dilakukan	Mengapa Penting?	Status
9	**Gunakan password yang kuat dan unik untuk setiap akun**	Password harus kombinasi huruf besar, huruf kecil, angka, dan simbol. Jangan pakai tanggal lahir atau nama	☐
10	**Aktifkan verifikasi dua langkah (Two-Factor Authentication)**	Lapisan keamanan tambahan yang meminta kode verifikasi saat login dari perangkat baru	☐
11	**Jangan posting foto anak dengan informasi sekolah atau lokasi**	Data anak sangat sensitif dan bisa disalahgunakan untuk penculikan atau eksploitasi	☐
12	**Matikan fitur lokasi atau GPS saat posting**	Penipu bisa melacak kebiasaan kita dan tahu kapan rumah kita kosong	☐
13	**Hati-hati saat menggunakan WiFi publik**	WiFi publik tidak aman. Jangan login ke mobile banking atau aplikasi penting saat pakai WiFi umum	☐
14	**Cek aktivitas login secara rutin**	Periksa apakah ada login mencurigakan dari lokasi atau perangkat yang tidak dikenal	☐
15	**Jangan klik link mencurigakan di DM atau komentar**	Link bisa mengarah ke situs phishing yang mencuri password kita	☐

💡 **Ingat Selalu**

Apa yang kita posting di media sosial bisa dilihat oleh siapa saja, termasuk penipu. Semakin banyak informasi pribadi yang kita bagikan, semakin mudah bagi penipu untuk menyamar menjadi kita atau memanfaatkan data kita untuk kejahatan. Lindungi diri dan keluarga dengan menerapkan checklist di atas mulai hari ini.

Rangkuman Modul 1

Setelah mempelajari Modul 1, sekarang Anda sudah memahami pentingnya menjaga data pribadi di era digital. Berikut adalah rangkuman singkat yang harus Anda ingat dan praktikkan setiap hari untuk melindungi diri dan keluarga dari kejahatan digital.

📌 5 Poin Kunci Jaga Data Pribadi

No.	Poin Kunci	Penjelasan Singkat	Contoh Praktis
1	**Jangan Pernah Berikan OTP, PIN, atau Password kepada Siapa Pun**	Kode OTP, PIN ATM, dan password adalah kunci pribadi Anda. Bank, polisi, atau petugas resmi tidak akan pernah meminta kode ini	Kalau ada yang telepon mengaku dari bank dan minta OTP, langsung tutup telepon dan hubungi bank langsung
2	**Hati-Hati dengan Link dan File APK dari Orang Tidak Dikenal**	File APK dan link mencurigakan bisa mencuri semua data di HP Anda. Jangan klik sembarangan	Kalau terima undangan pernikahan atau foto paket dengan format .apk, langsung hapus dan blokir
3	**Gunakan Password yang Kuat dan Aktifkan Autentikasi Dua Faktor**	Password harus kombinasi huruf besar, kecil, angka, dan simbol. Ganti secara berkala setiap 3-6 bulan. Aktifkan verifikasi dua langkah di semua akun penting	Jangan pakai tanggal lahir atau nama sebagai password. Contoh password kuat: R4h@s!a2025
4	**Jaga Privasi di Media Sosial**	Jangan posting foto KTP, boarding pass, tanggal lahir lengkap, atau alamat rumah. Atur akun menjadi "Pribadi" dan batasi siapa yang bisa lihat postingan Anda	Sebelum posting, tanya diri sendiri: "Apakah informasi ini aman kalau dilihat orang asing?"
5	**Hati-Hati dengan WiFi Umum dan Selalu Perbarui Aplikasi**	WiFi publik tidak aman. Jangan buka mobile banking atau masukkan data penting saat pakai WiFi umum. Selalu update aplikasi untuk menutup celah keamanan	Kalau terpaksa pakai WiFi umum, jangan login ke aplikasi bank atau e-wallet. Tunggu sampai pakai data seluler sendiri

💡 Ingat Selalu!

"Data Pribadi = Harta Karun. Jaga seperti Anda menjaga emas dan perhiasan."

Kejahatan digital bisa menimpa siapa saja, kapan saja. Tapi dengan menerapkan 5 poin kunci di atas, Anda sudah melangkah jauh untuk melindungi diri dan keluarga. Jangan tunggu sampai menjadi korban untuk mulai waspada. Mulai sekarang, jadikan keamanan data sebagai kebiasaan sehari-hari.

BAGIAN 4: MODUL 2 - CERDAS FINANSIAL, LAWAN PINJOL ILEGAL

Pinjol Legal vs Pinjol Ilegal

Apa Itu Fintech Peer-to-Peer Lending?

Fintech Peer-to-Peer Lending, atau sering disebut P2P Lending, adalah layanan pinjam-meminjam uang yang prosesnya menggunakan aplikasi atau website di internet. Di sini, ada tiga pihak yang terlibat: pemberi pinjaman (yang punya uang), peminjam (yang butuh uang), dan penyelenggara platform. Sistem ini mempertemukan pemberi dan penerima pinjaman secara langsung tanpa harus lewat bank. Semua layanan P2P Lending yang resmi wajib terdaftar dan punya izin dari OJK (Otoritas Jasa Keuangan). OJK bertugas mengawasi, memeriksa, dan memberi aturan agar proses pinjam-meminjam berjalan aman dan adil untuk semua pihak. Dengan pengawasan ini, bunga pinjaman, syarat, serta perlindungan nasabah semua sudah diatur supaya tidak merugikan masyarakat.

Apa Itu Pinjol Ilegal (Rentenir Online)?

Pinjol ilegal adalah layanan pinjaman online yang tidak terdaftar di OJK dan tidak mengikuti aturan pemerintah. Pinjol ilegal sering disebut juga rentenir online karena cara kerjanya seperti lintah darat: mereka menawarkan pinjaman dengan syarat mudah, tapi bunga dan denda sangat tinggi. Pinjol ilegal tidak punya alamat kantor yang jelas, tidak ada layanan pengaduan resmi, dan sering kali mengambil data pribadi peminjam tanpa izin lalu menyalahgunakannya untuk mengancam atau mempermalukan korban. Karena tidak diawasi, pinjol ilegal sangat berbahaya dan banyak menjerat masyarakat dengan utang yang makin lama makin besar. Jangan pernah pinjam uang dari pinjol ilegal, karena risikonya bukan hanya soal uang, tapi juga bisa membahayakan identitas dan nama baik keluarga.

Ciri-Ciri Pinjol Ilegal (Checklist)

Sebelum meminjam uang secara online, Anda harus tahu ciri-ciri pinjol ilegal agar tidak terjerat. Pinjol ilegal sangat berbahaya karena bisa membuat hidup Anda dan keluarga hancur. Berikut adalah ciri-ciri yang harus Anda waspadai.

⚠️ Checklist Ciri-Ciri Pinjol Ilegal

No.	Ciri-Ciri	Penjelasan	Tanda Bahaya
1	**Menawarkan pinjaman lewat SMS atau WhatsApp tanpa diminta**	Pinjol legal tidak pernah menawarkan pinjaman lewat SMS atau WhatsApp. Mereka hanya melayani orang yang datang sendiri ke aplikasi resmi mereka	🚨
2	**Bunga dan denda tidak jelas, sangat tinggi (1-4% per hari)**	Pinjol ilegal bisa mengenakan bunga 30-120% per bulan. Kalau pinjam Rp 1 juta, dalam sebulan bisa jadi Rp 2-3 juta	🚨🚨
3	**Syarat sangat mudah: cuma KTP dan selfie langsung cair**	Tidak ada pengecekan kemampuan bayar, tidak ada survei, bahkan orang yang sudah punya banyak utang tetap dikasih pinjaman	🚨
4	**Meminta akses seluruh data HP: Kontak, Galeri, Log Panggilan, Lokasi GPS**	Data ini digunakan untuk meneror kita dan keluarga kalau kita tidak bisa bayar. Foto kita bisa diedit jadi foto mesum lalu disebarkan ke semua kontak	🚨🚨🚨
5	**Alamat kantor tidak jelas atau fiktif**	Pinjol ilegal tidak punya kantor fisik yang bisa dikunjungi. Kalau ada masalah, kita tidak tahu harus melapor kemana	🚨
6	**Tidak terdaftar di OJK**	Ini ciri paling penting. Kalau tidak terdaftar di OJK, berarti ilegal dan tidak diawasi pemerintah	🚨🚨🚨
7	**Jangka waktu pelunasan sangat singkat (7-14 hari)**	Waktu bayar sangat pendek sehingga sulit untuk melunasi. Kalau telat sedikit saja, denda langsung membengkak	🚨🚨
8	**Tidak ada layanan pengaduan atau customer service**	Kalau ada masalah, nomor CS tidak aktif atau tidak bisa dihubungi. Kita tidak punya tempat mengadu	🚨
9	**Penagihan dengan cara teror, intimidasi, dan pelecehan**	Menelpon ratusan kali sehari, mengirim foto editan ke semua kontak, mengancam datang ke rumah atau kantor, bahkan ada yang sampai mengancam akan menyakiti keluarga	🚨🚨🚨

💡 **Ingat!**

Kalau ada salah satu ciri di atas, jangan pinjam! Pinjol ilegal akan membuat hidup Anda semakin susah. Lebih baik cari pinjaman dari keluarga, koperasi desa, atau pinjol legal yang terdaftar di OJK. Jangan sampai karena butuh uang cepat, Anda malah terjerat pinjol ilegal yang bisa menghancurkan kehidupan Anda dan keluarga.

Bahaya "Camilan" (Cepat, Mudah, Ngeri Belakangan)

Jebakan Kemudahan di Awal

Pinjol ilegal sengaja membuat proses pinjaman sangat cepat dan mudah agar orang tergiur. Mereka menawarkan dana cair dalam hitungan menit, cukup dengan KTP dan foto selfie, tanpa ribet mengisi formulir panjang atau survei lapangan. Ini adalah jebakan psikologis yang memanfaatkan kondisi orang yang sedang terdesak dan butuh uang cepat. Saat kita terpojok dan butuh uang secepatnya, kita cenderung tidak berpikir panjang tentang risikonya. Di awal, pinjol ilegal akan sangat ramah dan membuat kita merasa aman. Tapi begitu kita sudah memasang aplikasinya dan memberikan akses ke kontak, galeri, pesan, dan lokasi GPS kita, jebakan sudah terpasang. Aplikasi pinjol ilegal sebenarnya menyisipkan malware atau spyware yang diam-diam mencuri semua data pribadi kita. Sekali terjerat, pinjol ilegal bisa mengakses ribuan kontak dari satu peminjam saja, dan mereka akan menggunakan data itu untuk menawarkan pinjaman ke kontak kita atau sebagai senjata untuk meneror kita.

Risiko Penyebaran Data dan Ancaman

Yang paling mengerikan dari pinjol ilegal adalah praktik penyebaran data pribadi atau yang disebut doxing. Kalau kita telat bayar, meskipun hanya satu hari, pinjol ilegal akan langsung meneror kita dan menyebarkan informasi pribadi kita ke seluruh kontak di HP. Mereka akan mengirim pesan ke keluarga, teman, tetangga, bahkan atasan kita di kantor dengan isi yang mempermalukan seperti "Bapak Ahmad adalah penipu, tidak mau bayar utang" atau "Ibu Siti peminjam uang tidak bertanggung jawab". Lebih parah lagi, pinjol ilegal sering mengedit foto kita menjadi foto mesum atau foto yang melanggar kesusilaan, lalu disebarkan ke semua kontak dengan tujuan mempermalukan dan menekan kita agar segera bayar. Ancaman ini bisa berlangsung ratusan kali sehari lewat telepon dan pesan WhatsApp hingga malam hari. Banyak korban yang akhirnya mengalami depresi, dikucilkan oleh lingkungan, kehilangan pekerjaan, bahkan ada yang nekat bunuh diri karena tidak tahan dengan tekanan dan rasa malu. Ingat, penyebaran data pribadi tanpa izin adalah pelanggaran hukum yang dijerat dengan Pasal 26 UU ITE dan bisa dilaporkan ke polisi.

Cara Cek Legalitas Pinjol (Tutorial Praktis)

Sebelum meminjam uang di aplikasi pinjaman online, wajib hukumnya untuk mengecek apakah pinjol tersebut terdaftar resmi di OJK atau tidak. Jangan sampai Anda terjebak di pinjol ilegal yang akan membuat hidup semakin susah. Berikut adalah tiga cara mudah untuk mengecek legalitas pinjol.

🔍 Tiga Cara Mudah Cek Legalitas Pinjol

Cara	Langkah-Langkah	Kelebihan
1. Via WhatsApp OJK	1. Simpan nomor WhatsApp OJK: **081-157-157-157** 2. Buka WhatsApp dan chat ke nomor tersebut 3. Ketik nama aplikasi pinjol yang ingin dicek 4. Tunggu beberapa saat, OJK akan membalas apakah pinjol tersebut terdaftar atau tidak	Paling cepat dan mudah. Bisa dilakukan kapan saja tanpa buka website
2. Via Website OJK	1. Buka browser di HP atau komputer 2. Kunjungi website: **www.ojk.go.id** 3. Cari menu "Fintech Lending" atau "Direktori P2P Lending" 4. Lihat daftar lengkap pinjol legal yang terdaftar 5. Cari nama aplikasi yang ingin Anda cek	Bisa melihat daftar lengkap semua pinjol legal sekaligus
3. Via Telepon 157	1. Hubungi nomor **157** dari HP Anda 2. Ikuti petunjuk operator OJK 3. Tanyakan nama aplikasi pinjol yang ingin dicek 4. Petugas akan memberikan informasi legalitas	Bisa bertanya langsung dan konsultasi masalah keuangan lainnya

📋 Contoh Cara Pengecekan via WhatsApp

Chat dengan: 081-157-157-157 (OJK)

Anda: Min mau tanya, Apakah aplikasi "KreditPro" terdaftar di OJK?

OJK (Bot):
Terima kasih telah menghubungi OJK 157.
Kami sedang memeriksa data...

OJK (Bot):
Aplikasi "KreditPro" TIDAK TERDAFTAR di OJK.
⚠️ HATI-HATI! Ini adalah pinjol ilegal.
Jangan meminjam uang di aplikasi tersebut.

Untuk daftar pinjol legal, silakan kunjungi:
www.ojk.go.id

💡 Tips Penting

- **Cek sebelum memasang aplikasi**, bukan setelah sudah pinjam
- **Jangan percaya klaim "Terdaftar OJK"** yang ada di aplikasi atau iklan. Harus dicek sendiri ke sumber resmi OJK
- **Simpan nomor WhatsApp OJK (081-157-157-157)** di kontak HP Anda agar mudah dihubungi kapan saja
- **Kalau ragu, jangan pinjam!** Lebih baik cari alternatif lain seperti koperasi atau pinjam ke keluarga

⚠️ Ingat!

Per November 2025, hanya ada sekitar 102 pinjol legal yang terdaftar di OJK. Sisanya yang ratusan bahkan ribuan adalah pinjol ilegal yang sangat berbahaya. Jangan malas untuk melakukan pengecekan beberapa menit saja, karena bisa menyelamatkan hidup Anda dan keluarga dari jeratan pinjol ilegal.

Strategi Jika Terlanjur Terjerat (Bagian 1)

Tenangkan Diri, Jangan Panik

Kalau Anda sudah terlanjur meminjam di pinjol ilegal, hal pertama yang harus dilakukan adalah menenangkan diri dan jangan panik. Panik hanya akan membuat Anda mengambil keputusan yang salah dan memperburuk situasi. Pahami bahwa Anda tidak sendirian, ribuan orang lain juga mengalami hal yang sama dan banyak yang berhasil keluar dari jeratan ini. Yang paling penting, jangan pernah gali lubang tutup lubang, yaitu meminjam uang dari pinjol lain untuk membayar utang pinjol sebelumnya. Ini adalah kesalahan fatal yang akan membuat Anda terperosok lebih dalam ke dalam pusaran utang yang tidak akan pernah selesai. Setiap pinjol ilegal baru yang Anda ambil akan mencuri data Anda lagi, dan teror akan berlipat ganda. Fokuskan energi Anda untuk menyelesaikan masalah yang ada, bukan menambah masalah baru.

Lunasi Pokok Utang Jika Mampu, Negosiasi Bunga yang Tidak Masuk Akal

Langkah kedua adalah mengevaluasi kemampuan finansial Anda. Jika Anda mampu, segera lunasi hanya utang pokok saja (jumlah uang yang benar-benar Anda terima di awal). Anda tidak wajib membayar bunga yang tidak masuk akal, denda yang mencekik, atau biaya-biaya tambahan lain yang tidak jelas. Menurut OJK dan ahli hukum, ada kewajiban moral dan hukum perdata untuk mengembalikan sejumlah uang pokok yang telah Anda terima, tapi bunga dan denda dari pinjol ilegal tidak memiliki dasar hukum yang kuat. Jika Anda tidak mampu melunasi sekaligus, coba lakukan negosiasi dengan pihak pinjol. Ajukan keringanan seperti perpanjangan waktu pembayaran, pengurangan bunga, atau cicilan yang lebih kecil. Tunjukkan itikad baik Anda untuk membayar dengan membuat kesepakatan tertulis. Namun ingat, jangan sampai Anda dipaksa membayar jumlah yang tidak wajar. Prioritaskan membayar utang dari gaji atau hasil menjual aset yang tidak terlalu penting, bukan dengan membuat utang baru.

Strategi Menghadapi Teror (Bagian 2)

Blokir dan Informasikan ke Keluarga

Jika Anda sudah mulai mengalami teror dari debt collector pinjol ilegal, langkah pertama adalah blokir semua nomor penagih yang kasar, mengancam, atau mempermalukan Anda. Anda tidak wajib menerima telepon atau pesan yang berisi ancaman, kata-kata kotor, atau intimidasi. Debt collector yang profesional dan legal tidak akan menggunakan cara-cara seperti itu. Langkah penting berikutnya adalah segera menginformasikan kepada keluarga, teman dekat, dan kontak darurat bahwa data pribadi Anda telah disalahgunakan oleh pinjol ilegal. Beritahu mereka untuk tidak merespons, tidak percaya, dan langsung memblokir setiap panggilan atau pesan dari pihak yang mengaku debt collector. Jelaskan bahwa pinjol ilegal

sering mengedit foto dan menyebar informasi palsu untuk mempermalukan korban. Dengan memberitahu keluarga lebih dulu, Anda sudah menutup celah psikologis yang biasa dipakai pinjol ilegal untuk menekan korban.

Kumpulkan Bukti untuk Pelaporan

Langkah paling krusial adalah mengumpulkan semua bukti teror yang Anda terima. Simpan semua bukti interaksi dengan pinjol ilegal secara rapi dan sistematis, termasuk:

- Screenshot semua chat atau pesan WhatsApp yang berisi ancaman, kata kasar, atau penyebaran foto/informasi pribadi
- Rekaman percakapan telepon yang berisi intimidasi atau teror (jika memungkinkan)
- Screenshot atau foto pesan yang disebarkan ke kontak keluarga dan teman
- Bukti transfer pembayaran yang sudah dilakukan (jika ada)
- Screenshot aplikasi dan informasi pinjol ilegal

Bukti-bukti ini sangat penting untuk melaporkan pinjol ilegal ke OJK, Kominfo, dan Kepolisian. Dengan adanya bukti yang kuat, pihak berwenang bisa melacak dan menindak pinjol ilegal secara hukum. Ingat, penyebaran data pribadi dan ancaman adalah tindak pidana yang bisa dijerat dengan UU ITE. Anda adalah korban, bukan penjahat, jadi jangan takut untuk melaporkan.

Simulasi Role-Playing: Merespon Penagih (Skenario A)

Menghadapi debt collector pinjol ilegal yang kasar dan mengancam memang tidak mudah. Tapi dengan persiapan yang tepat dan kata-kata yang tegas namun sopan, Anda bisa melindungi diri dan menyampaikan bahwa Anda tahu hak-hak Anda. Berikut adalah simulasi percakapan yang bisa Anda pelajari dan praktikkan.

📞 **Situasi: Penagih Menelpon dengan Kata-Kata Kasar dan Ancaman**

☎️ **Panggilan Masuk: 0812-XXXX-XXXX (Debt Collector)**

Penagih: "Halo! Kamu utang Rp 5 juta belum bayar!
Kalau tidak bayar sekarang, aku sebar
foto kamu ke semua kontak! Mau dipermalukan?"

❌ **JANGAN JAWAB SEPERTI INI:**
"Maaf Pak, saya lagi tidak punya uang... tunggu
sebentar ya... jangan sebar data saya..."
(Ini menunjukkan Anda takut dan lemah)

✅ **JAWAB SEPERTI INI:**

> "Saya merekam percakapan ini untuk bukti. Saya tahu perusahaan Anda tidak terdaftar di OJK, jadi ini ILEGAL. Saya bersedia membayar POKOK pinjaman saja, bukan bunga yang tidak masuk akal. Kalau Anda menyebar data pribadi saya atau memfitnah saya, itu melanggar UU ITE Pasal 27 dan Pasal 32. Saya akan lapor ke OJK dan Polisi, dan saya TIDAK akan membayar sepeserpun."

📝 **Penjelasan Script Jawaban**

Bagian Script	Mengapa Penting?
"Saya merekam percakapan ini untuk bukti"	Memberi sinyal bahwa Anda siap melakukan tindakan hukum. Penagih akan berpikir dua kali sebelum mengancam lebih lanjut
"Perusahaan Anda tidak terdaftar di OJK, jadi ILEGAL"	Menunjukkan bahwa Anda paham hukum dan tahu bahwa mereka beroperasi secara ilegal
"Saya bersedia membayar POKOK pinjaman saja"	Menunjukkan itikad baik Anda untuk mengembalikan uang yang memang Anda pinjam, tapi tidak mau ditipu dengan bunga tinggi
"Menyebar data melanggar UU ITE Pasal 27 dan 32"	Memberi peringatan hukum yang konkret. Penyebaran data pribadi tanpa izin bisa dipidana hingga 6 tahun penjara
"Saya akan lapor ke OJK dan Polisi"	Ancaman balik yang legal dan sah. Anda punya hak untuk melaporkan mereka
"TIDAK akan membayar sepeserpun"	Memberi konsekuensi tegas jika mereka tetap melakukan intimidasi

💪 Tips Tambahan Saat Berbicara dengan Penagih

1. **Tetap Tenang dan Tegas**
   Jangan panik atau menangis. Bicara dengan nada datar dan tegas. Ingat, mereka mencoba menakut-nakuti Anda agar panik dan terburu-buru membayar.

2. **Jangan Terpancing Emosi**
   Kalau mereka marah atau menghina, tetap tenang. Jangan balas dengan emosi karena itu yang mereka inginkan. Ulangi script di atas dengan tenang.

3. **Catat Nama dan Nomor Penagih**
   Tanya identitas lengkap mereka: nama, nomor karyawan, dari perusahaan apa. Biasanya penagih pinjol ilegal tidak berani memberikan identitas asli.

4. **Akhiri Percakapan dengan Tegas**
   Setelah menyampaikan script di atas, katakan: "Saya sudah sampaikan posisi saya. Terima kasih." Lalu tutup telepon. Jangan berdebat panjang lebar.

5. **Segera Blokir Nomor Setelah Merekam**
   Setelah percakapan selesai dan Anda sudah punya rekaman, langsung blokir nomor tersebut. Tidak ada gunanya terus menerima telepon yang sama.

⚖️ **Dasar Hukum yang Anda Miliki**

- **UU ITE Pasal 27 ayat (3)**: Pelanggaran terhadap pencemaran nama baik dan fitnah bisa dipidana 4 tahun penjara
- **UU ITE Pasal 32**: Penyebaran data pribadi tanpa izin bisa dipidana 6 tahun penjara
- **UU Perlindungan Data Pribadi (UU PDP)**: Melindungi hak Anda atas data pribadi

💡 **Ingat:** Anda adalah KORBAN, bukan penjahat. Pinjol ilegal yang melanggar hukum, bukan Anda. Jangan takut untuk bersikap tegas dan melaporkan mereka.

Simulasi Role-Playing: Merespon Penagih (Skenario B)

Salah satu taktik paling menjengkelkan dari pinjol ilegal adalah meneror kontak darurat atau orang-orang di daftar kontak peminjam. Kalau Anda menerima telepon atau pesan dari debt collector yang menagih utang orang lain, Anda harus tahu bahwa **Anda TIDAK berkewajiban membayar utang tersebut**. Berikut adalah simulasi bagaimana merespons dengan benar.

📞 Situasi: Penagih Meneror Kontak Darurat (Teman/Bos)

☎️ Panggilan Masuk ke Teman/Rekan Kerja

> Penagih: "Halo, Anda kenal Ahmad? Dia utang Rp 10 juta di perusahaan kami. Tolong sampaikan dia harus bayar sekarang atau Anda yang akan kami tagih!"

❌ JANGAN JAWAB SEPERTI INI:
"Oh iya, saya kenal Ahmad. Baik, nanti saya sampaikan ke dia ya Pak..."
(Ini membuat penagih terus menghubungi Anda)

✅ JAWAB SEPERTI INI:
"Saya tidak ada sangkut pautnya dengan utang ini. Saya BUKAN penanggung jawab dan TIDAK WAJIB membayar utang orang lain. Menurut Surat Edaran OJK Nomor 19 Tahun 2023, kontak darurat TIDAK BOLEH dijadikan sasaran penagihan. Jangan hubungi saya lagi atau saya akan laporkan nomor Anda ke OJK dan Polisi sebagai gangguan dan intimidasi."

📝 Penjelasan Script Jawaban untuk Kontak Darurat

Bagian Script	Mengapa Penting?
"Saya tidak ada sangkut pautnya dengan utang ini"	Menegaskan bahwa Anda bukan pihak yang berutang dan tidak punya tanggung jawab hukum apapun
"Saya BUKAN penanggung jawab"	Kontak darurat bukan penjamin atau penanggung utang. Secara hukum, Anda tidak wajib membayar
"SE OJK Nomor 19 Tahun 2023: kontak darurat TIDAK BOLEH dijadikan sasaran penagihan"	Ini adalah dasar hukum yang jelas. Pinjol legal tidak boleh menagih ke kontak darurat, apalagi pinjol ilegal
"Jangan hubungi saya lagi"	Perintah tegas yang menunjukkan Anda tidak akan terlibat dalam masalah ini

Bagian Script	Mengapa Penting?
"Saya akan laporkan ke OJK dan Polisi sebagai gangguan"	Ancaman hukum yang sah. Mengganggu orang yang bukan debitur adalah pelanggaran

💪 Langkah-Langkah untuk Kontak Darurat yang Diteror

1. Tetap Tenang dan Tegas

Jangan merasa bersalah atau bertanggung jawab. Utang bukan tanggung jawab Anda.

2. Tolak Semua Permintaan Pembayaran

Jangan pernah membayar utang orang lain, meskipun itu teman atau keluarga dekat. Kalau Anda bayar, Anda akan dianggap sebagai penanggung dan akan terus ditagih.

3. Blokir Nomor Penagih

Setelah menyampaikan script di atas sekali, langsung blokir nomor tersebut. Tidak ada gunanya berdebat lebih lanjut.

4. Simpan Bukti Teror

Screenshot semua chat dan rekam percakapan telepon sebagai bukti kalau Anda perlu melaporkan.

5. Laporkan ke Pihak Berwenang

Anda bisa melaporkan ke:

- **OJK**: Melalui website sipasti.ojk.go.id atau WhatsApp 081-157-157-157
- **AFPI** (untuk fintech legal): Melalui website fintech.id
- **Polisi**: Kalau sudah ada ancaman atau intimidasi serius

6. Beritahu Peminjam

Kalau Anda kenal dengan orang yang meminjam, beritahu dia bahwa Anda sudah dihubungi oleh debt collector dan minta dia untuk menyelesaikan masalahnya sendiri tanpa melibatkan Anda.

⚖️ Hak-Hak Kontak Darurat

Menurut Surat Edaran OJK Nomor 19 Tahun 2023:

- Kontak darurat **HANYA** untuk konfirmasi keberadaan peminjam, **BUKAN** untuk penagihan
- Pinjol **WAJIB** meminta izin terlebih dahulu kepada kontak darurat sebelum mencantumkan nomor mereka
- Penagihan **TIDAK BOLEH** dilakukan dengan cara intimidatif, ancaman, atau menyebarkan informasi pribadi
- Kontak darurat **BERHAK** menolak dihubungi dan melaporkan pinjol yang melanggar aturan

📣 Pesan untuk Kontak Darurat

🚨 **INGAT!**

Anda BUKAN penanggung jawab utang orang lain.
Kontak darurat ≠ Penjamin utang.

Jangan merasa bersalah.
Jangan bayarkan utang orang lain.
Langsung blokir dan laporkan!

Hubungi OJK: 081-157-157-157
atau sipasti.ojk.go.id

💡 **Untuk Peminjam:** Jangan pernah memasukkan nomor orang lain sebagai kontak darurat tanpa izin mereka. Ini akan merugikan orang yang Anda cantumkan dan membuat hubungan Anda dengan mereka rusak.

Fatwa dan Pandangan Hukum

Sebelum membahas lebih jauh tentang pinjol ilegal, penting bagi Anda untuk memahami status hukum pinjaman online ilegal di Indonesia. Memahami dasar hukumnya akan membuat Anda lebih percaya diri dalam melawan praktik pinjol ilegal yang merugikan.

Status Hukum Perjanjian Pinjol Ilegal (Hukum Perdata)

Secara hukum perdata, perjanjian pinjam meminjam dengan pinjol ilegal tidak sah dan dapat dibatalkan. Mengapa demikian? Karena perjanjian tersebut tidak memenuhi syarat sahnya perjanjian menurut Pasal 1320 KUH Perdata. Pasal 1320 KUH Perdata menyebutkan bahwa

untuk sahnya suatu perjanjian diperlukan empat syarat, yaitu: (1) kesepakatan para pihak, (2) kecakapan untuk membuat perjanjian, (3) suatu hal tertentu, dan (4) suatu sebab yang halal. Pinjol ilegal melanggar syarat keempat, yaitu sebab yang halal, karena kegiatan pinjol ilegal dilarang oleh undang-undang dan bertentangan dengan ketertiban umum.

Berdasarkan Pasal 1337 KUH Perdata, suatu sebab adalah terlarang apabila sebab tersebut dilarang oleh undang-undang atau bertentangan dengan kesusilaan maupun ketertiban umum. Karena pinjol ilegal tidak memiliki izin dari OJK dan beroperasi melanggar hukum, maka perjanjiannya dianggap batal demi hukum atau dapat dibatalkan. Akibatnya, pinjol ilegal tidak bisa menempuh jalur hukum yang sah (seperti gugatan di pengadilan) untuk menagih utang tersebut. Meski demikian, secara moral dan hukum perdata, Anda tetap memiliki kewajiban untuk mengembalikan uang pokok yang benar-benar Anda terima, bukan bunga dan denda yang tidak masuk akal. Namun, jika Anda dipaksa membayar dengan cara yang melanggar hukum seperti teror, ancaman, dan penyebaran data pribadi, OJK mendorong masyarakat untuk melaporkan dan tidak membayar.

Aspek Pidana Bagi Penagih yang Mengancam (UU ITE)

Dari sisi hukum pidana, aktivitas pinjol ilegal dan penagihan dengan cara mengancam atau intimidasi termasuk tindak pidana yang bisa dijerat dengan berbagai pasal. Penagih utang pinjol ilegal yang melakukan teror, ancaman, penyebaran data pribadi, atau mempermalukan korban dapat dikenai sanksi pidana berdasarkan:

1. Undang-Undang ITE (Informasi dan Transaksi Elektronik)

Pasal 27 ayat (3) tentang pencemaran nama baik dan penghinaan: Ancaman pidana penjara maksimal 4 tahun dan/atau denda maksimal Rp 750 juta

Pasal 29 tentang ancaman kekerasan melalui media elektronik: Ancaman pidana penjara maksimal 12 tahun dan/atau denda maksimal Rp 2 miliar

Pasal 32 tentang penyebaran data pribadi tanpa izin: Ancaman pidana penjara maksimal 8 tahun dan/atau denda maksimal Rp 2 miliar

2. KUHP (Kitab Undang-Undang Hukum Pidana)

Pasal 335 tentang perbuatan tidak menyenangkan

Pasal 368 tentang pemerasan dan ancaman: Ancaman pidana penjara maksimal 9 tahun

3. UU Perlindungan Konsumen

Pinjol ilegal melanggar Pasal 8 ayat (1) huruf a tentang penyediaan jasa yang tidak memenuhi standar dan ketentuan perundang-undangan.

Pemerintah melalui OJK, Polri, dan Kementerian Komunikasi dan Digital telah membentuk Tim Pokja (Kelompok Kerja) untuk menindak tegas pinjol ilegal. Sejak 2018, pemerintah telah memblokir lebih dari 6.000 aplikasi dan website pinjol ilegal. Kepala Kepolisian RI juga diberikan kewenangan penuh untuk mengambil langkah hukum sesuai dengan Pasal 213 Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan untuk menindak pelaku pinjol ilegal.

Kesimpulan Hukum

Anda perlu tahu:

- Perjanjian dengan pinjol ilegal tidak sah secara hukum
- Anda hanya wajib mengembalikan pokok utang, bukan bunga dan denda yang tidak wajar
- Penagih yang mengancam, menyebar data pribadi, atau mempermalukan Anda melanggar hukum pidana dan bisa dilaporkan ke polisi
- Pinjol ilegal tidak bisa menggugat Anda ke pengadilan karena perjanjiannya tidak sah
- Anda berhak melaporkan pinjol ilegal ke OJK, Kominfo, dan Polisi tanpa takut

💡 Ingat: Hukum melindungi korban pinjol ilegal, bukan pelakunya. Jangan takut untuk melaporkan dan memperjuangkan hak Anda !

Rangkuman Modul 2

Setelah mempelajari Modul 2 tentang pinjol legal vs pinjol ilegal, sekarang Anda sudah memahami bahaya pinjol ilegal dan bagaimana cara melindungi diri. Berikut adalah rangkuman singkat yang harus Anda ingat dan praktikkan untuk menjadi warga digital yang cerdas dalam keuangan.

🔑 LANGKAH "3C" AMAN BERMAIN PINJOL

Untuk memastikan Anda terhindar dari jebakan pinjol ilegal, ingat selalu **Langkah 3C** sebelum meminjam uang secara online:

3C	Penjelasan	Cara Melakukannya
1. CEK LEGALITAS	Pastikan pinjol terdaftar dan berizin resmi di OJK	- Buka WhatsApp dan chat ke **081-157-157-157** (OJK) - Ketik nama aplikasi pinjol yang ingin dicek - Atau kunjungi website **www.ojk.go.id** untuk lihat daftar lengkap pinjol legal - Atau hubungi **157** dari HP Anda - Jangan percaya klaim "Terdaftar OJK" yang ada di iklan. Harus dicek sendiri!
2. CERMATI SYARAT	Baca dan pahami semua syarat, bunga, denda, dan biaya tersembunyi dengan teliti	- Jangan asal klik "Setuju" tanpa membaca perjanjian digital - Pastikan bunga pinjaman tidak lebih dari 0,4% per hari (maksimal 146% per tahun) sesuai aturan OJK - Tanyakan semua biaya: admin, provisi, asuransi, denda keterlambatan - Pastikan tenor (jangka waktu) realistis untuk kemampuan Anda - Jangan tergiur bunga rendah tapi banyak biaya tersembunyi
3. CICIL SESUAI KEMAMPUAN	Pinjam hanya sesuai kebutuhan dan pastikan cicilan tidak lebih dari 30% dari pendapatan bulanan Anda	- Hitung penghasilan bersih Anda per bulan - Cicilan maksimal = 30% dari gaji - Contoh: Gaji Rp 3 juta, maka cicilan maksimal Rp 900 ribu/bulan - Jangan pinjam untuk hal yang tidak mendesak atau untuk bergaya hidup - Jangan gali lubang tutup lubang (pinjam baru untuk bayar utang lama)

📋 CHECKLIST SEBELUM MEMINJAM DI PINJOL

Centang semua poin di bawah ini sebelum meminjam:

Status	Pertanyaan Penting
☐	Apakah pinjol ini sudah saya cek legalitasnya di WhatsApp OJK 081-157-157-157?
☐	Apakah pinjol ini terdaftar resmi di OJK?
☐	Apakah saya sudah membaca dan memahami semua syarat dan ketentuan?
☐	Apakah bunga dan biaya yang dikenakan wajar dan transparan?
☐	Apakah cicilan bulanan tidak lebih dari 30% gaji saya?
☐	Apakah saya benar-benar membutuhkan pinjaman ini untuk hal yang mendesak?
☐	Apakah saya punya rencana pembayaran yang jelas?
☐	Apakah pinjol ini hanya meminta akses kamera dan lokasi saja (bukan kontak, galeri, atau pesan)?
☐	Apakah aplikasi ini diunduh dari Google Play Store atau Apple App Store (bukan file APK dari WhatsApp)?
☐	Apakah saya sudah memberitahu keluarga bahwa saya mengajukan pinjaman ini?

Kalau ada satu saja yang tidak dicentang atau jawabannya "Tidak", JANGAN PINJAM!

⚠️ INGAT SELALU: CAMILAN (Cepat, Mudah, Ngeri Belakangan)

Pinjol ilegal sengaja membuat proses pinjaman **cepat dan mudah** untuk menarik korban. Tapi yang harus Anda ingat adalah dampaknya yang **ngeri di belakangan**:

- Data pribadi disebarkan ke semua kontak
- Teror dan ancaman setiap hari

- Foto pribadi diedit jadi foto mesum
- Bunga dan denda membengkak tidak masuk akal
- Nama baik rusak di lingkungan

Jangan tergiur kemudahan sesaat yang akan membuat hidup Anda hancur!

💡 ALTERNATIF SELAIN PINJOL

Sebelum memutuskan meminjam di pinjol, pertimbangkan alternatif lain yang lebih aman:

1. **Pinjam ke keluarga atau teman dekat** dengan perjanjian yang jelas
2. **Koperasi desa atau koperasi simpan pinjam** dengan bunga yang wajar
3. **Bank dengan KTA (Kredit Tanpa Agunan)** untuk pinjaman yang lebih besar
4. **Menunda pembelian** yang tidak mendesak
5. **Jual aset yang tidak terpakai** seperti HP lama, motor, atau perhiasan

🎯 PESAN PENUTUP MODUL 2

"Jangan pernah meminjam uang karena gaya hidup. Pinjam hanya untuk kebutuhan mendesak dan produktif."

Pinjaman online yang aman adalah pinjaman yang:

- ✅ Terdaftar di OJK
- ✅ Transparan biaya dan bunganya
- ✅ Sesuai dengan kemampuan bayar Anda
- ✅ Untuk kebutuhan yang benar-benar mendesak

Ingat Langkah 3C:

1. **CEK** legalitas di OJK
2. **CERMATI** syarat dan bunga
3. **CICIL** sesuai kemampuan (maksimal 30% dari gaji)

Dengan menerapkan Langkah 3C, Anda akan terhindar dari jeratan pinjol

BAGIAN 5: PENUTUP & REFERENSI

Checklist Keamanan Digital (Lembar Potong/Copy)

Gunakan checklist ini sebagai panduan untuk memastikan Anda dan keluarga terlindungi dari kejahatan digital dan pinjol ilegal. Centang setiap poin yang sudah Anda lakukan, dan segera lakukan poin yang belum tercentang.

✅ CHECKLIST KEAMANAN DIGITAL SAYA

Petunjuk: Centang (✓) setiap poin yang sudah Anda lakukan

A. KEAMANAN AKUN DAN PASSWORD

Status	Tindakan yang Harus Dilakukan
☐	Sudah mengganti password semua akun penting (email, mobile banking, media sosial) dalam 3 bulan terakhir
☐	Menggunakan password yang kuat: kombinasi huruf besar, kecil, angka, dan simbol (minimal 8 karakter)
☐	Tidak menggunakan password yang sama untuk beberapa akun
☐	Sudah mengaktifkan verifikasi dua langkah (2FA) di semua akun penting
☐	Tidak pernah memberikan kode OTP, PIN, atau password kepada siapa pun

B. KEAMANAN MEDIA SOSIAL

Status	Tindakan yang Harus Dilakukan
☐	Mengatur akun media sosial menjadi "Pribadi" atau "Teman Saja"
☐	Tidak pernah memposting foto KTP, SIM, atau dokumen identitas
☐	Tidak pernah memposting tiket pesawat (boarding pass)
☐	Menyembunyikan tanggal lahir lengkap dan alamat rumah di media sosial

Status	Tindakan yang Harus Dilakukan
☐	Tidak sembarangan menerima permintaan pertemanan dari orang asing
☐	Mematikan fitur lokasi/GPS saat memposting di media sosial

C. KEAMANAN APLIKASI DAN HP

Status	Tindakan yang Harus Dilakukan
☐	Memeriksa dan mengatur izin akses aplikasi di HP (kontak, galeri, lokasi, kamera)
☐	Tidak pernah memasang file APK dari WhatsApp atau SMS
☐	Mengunduh aplikasi hanya dari Google Play Store atau Apple App Store
☐	Melakukan backup kontak dan data penting ke cloud secara rutin
☐	Menghapus aplikasi yang sudah tidak digunakan secara berkala (setiap 2-3 bulan)
☐	Menggunakan aplikasi pengaman data seperti Norton atau Avast Mobile Security

D. KEAMANAN DARI PHISHING DAN PENIPUAN

Status	Tindakan yang Harus Dilakukan
☐	Tidak pernah mengklik link mencurigakan dari SMS, WhatsApp, atau email
☐	Tidak pernah memberikan data pribadi ke situs yang tidak aman (tanpa HTTPS)
☐	Selalu mengecek nomor pengirim sebelum merespons pesan atau telepon
☐	Tidak menggunakan WiFi publik untuk mengakses mobile banking atau aplikasi keuangan
☐	Memblokir dan melaporkan nomor atau akun yang mencurigakan

E. KEAMANAN DARI PINJOL ILEGAL

Status	Tindakan yang Harus Dilakukan
☐	Sudah menyimpan nomor WhatsApp OJK (081-157-157-157) di kontak HP
☐	Sudah mengecek legalitas pinjol di WhatsApp OJK atau website OJK sebelum meminjam

Status	Tindakan yang Harus Dilakukan
☐	Tidak pernah meminjam uang dari aplikasi yang menawarkan pinjaman lewat SMS/WhatsApp
☐	Tidak pernah memberikan izin akses kontak, galeri, dan log panggilan ke aplikasi pinjol
☐	Menginformasikan keluarga dan teman dekat untuk tidak merespons debt collector pinjol ilegal
☐	Memahami bahwa saya hanya wajib bayar pokok utang pinjol ilegal, bukan bunga tinggi
☐	Menyimpan bukti teror (screenshot, rekaman) untuk pelaporan

F. TINDAKAN DARURAT JIKA TERJADI MASALAH

Status	Tindakan yang Harus Dilakukan
☐	Tahu cara melaporkan ke OJK: WhatsApp 081-157-157-157 atau sipasti.ojk.go.id
☐	Tahu cara melaporkan ke Polisi jika mengalami ancaman atau intimidasi
☐	Tahu cara memblokir aplikasi yang mencuri data pribadi
☐	Memiliki kontak darurat yang terpercaya untuk dimintai bantuan

📊 Skor Keamanan Digital Anda

Hitung berapa poin yang sudah Anda centang:

Jumlah Centang	Status Keamanan	Tindakan
30-35	🟢 **Sangat Aman**	Pertahankan! Anda sudah melindungi diri dengan baik
20-29	🟡 **Cukup Aman**	Segera lakukan poin yang belum tercentang
10-19	🟠 **Kurang Aman**	Prioritaskan bagian A, D, dan E untuk segera dilakukan
0-9	🔴 **Sangat Berisiko**	Segera lakukan semua poin, dimulai dari yang paling penting

💡 Catatan Penting

✂️ **Potong atau fotokopi halaman ini dan tempelkan di tempat yang mudah terlihat (kulkas, meja kerja, dinding kamar)**

📱 **Atau foto halaman ini dan simpan di galeri HP Anda sebagai pengingat**

🔄 **Lakukan evaluasi ulang setiap 3 bulan sekali untuk memastikan keamanan tetap terjaga**

Ingat: Keamanan digital bukan sesuatu yang dilakukan sekali lalu selesai, tapi kebiasaan yang harus dipraktikkan setiap hari. Dengan mencentang semua poin di atas, Anda sudah melangkah jauh untuk melindungi diri, keluarga, dan data pribadi dari kejahatan digital.

Kontak Penting & Kanal Pengaduan

Jika Anda menjadi korban kejahatan digital, pinjol ilegal, atau menemukan konten ilegal di internet, jangan diam saja. Segera laporkan ke pihak berwenang menggunakan kontak di bawah ini. Simpan halaman ini atau foto halaman ini agar mudah diakses saat dibutuhkan.

📞 DAFTAR KONTAK PENGADUAN RESMI

Lembaga	Untuk Melaporkan Apa?	Cara Menghubungi
Otoritas Jasa Keuangan (OJK)	- Pinjol ilegal - Penagihan yang kasar dan intimidatif - Penyalahgunaan data pribadi oleh fintech - Investasi bodong	**Telepon:** 157 (gratis dari HP) **WhatsApp:** 081-157-157-157 **Website:** sipasti.ojk.go.id **Email:** konsumen@ojk.go.id [^1]
Kementerian Komunikasi dan Digital (Kominfo)	- Situs atau aplikasi pinjol ilegal - Konten penipuan online - Judi online - Pornografi - Hoaks dan berita bohong - Pelanggaran UU ITE	**Website:** aduankonten.id **WhatsApp:** 081-1922-4545 **Email:** aduankonten@komdigi.go.id **Cek Rekening:** cekrekening.id

Lembaga	Untuk Melaporkan Apa?	Cara Menghubungi
Kepolisian Republik Indonesia (Polri)	- Ancaman dan intimidasi - Pencemaran nama baik - Penyebaran foto/data pribadi tanpa izin - Pemerasan dan pemerasan online - Segala bentuk kejahatan siber	**Website:** patrolisiber.id **Email:** polisionline.net@gmail.com **Telepon Darurat:** 110 **Atau datang ke kantor polisi terdekat**
Satuan Tugas Waspada Investasi (Satgas WI)	- Investasi bodong - Penawaran investasi ilegal - Penipuan berkedok investasi - Robot trading palsu - MLM ilegal	**Website:** waspadainvestasi.ojk.go.id **Telepon:** 157 (hubungi OJK) **Email:** waspadainvestasi@ojk.go.id

📝 CARA MELAPORKAN KE MASING-MASING LEMBAGA

A. Melaporkan ke OJK (Pinjol Ilegal & Fintech)

Langkah-langkah:

1. Siapkan bukti: screenshot chat ancaman, bukti transfer, rekaman suara, nama aplikasi pinjol
2. Hubungi OJK via WhatsApp 081-157-157-157 atau kunjungi sipasti.ojk.go.id
3. Isi formulir pengaduan dengan lengkap: nama, kontak, kronologi masalah
4. Upload semua bukti yang sudah disiapkan
5. Tunggu nomor tiket pengaduan untuk lacak status laporan Anda
6. OJK akan merespons dalam 2-10 hari kerja

Yang perlu dilampirkan:

- Identitas pelapor (KTP)
- Screenshot aplikasi pinjol ilegal
- Bukti transaksi atau pinjaman
- Screenshot ancaman atau teror
- Nomor telepon penagih yang mengganggu

B. Melaporkan ke Kominfo (Situs/Aplikasi Ilegal)

Langkah-langkah:

1. Kunjungi website aduankonten.id
2. Daftar atau login jika sudah punya akun
3. Klik "Buat Aduan Baru"
4. Pilih kategori: Penipuan Online / Investasi Ilegal / Judi Online / Aplikasi Ilegal
5. Masukkan URL atau link situs/aplikasi yang dilaporkan
6. Upload screenshot sebagai bukti
7. Tulis alasan pelaporan dengan jelas
8. Kirim aduan dan catat nomor tiket untuk lacak progres

Atau via WhatsApp: 081-1922-4545

Yang bisa dilaporkan:

- Situs pinjol ilegal
- Aplikasi penipuan online
- Judi online
- Pornografi
- Hoaks dan berita bohong
- Investasi bodong
- Obat ilegal
- Pelanggaran UU ITE

Proses: Tim Kominfo akan verifikasi dalam 1x24 sampai 2x24 jam. Jika terbukti ilegal, situs akan diblokir

C. Melaporkan ke Polisi (Kejahatan Siber)

Langkah-langkah:

1. Kunjungi website patrolisiber.id atau datang langsung ke kantor polisi terdekat
2. Bawa semua bukti: print screenshot, rekaman percakapan, bukti transfer
3. Buat Surat Tanda Penerimaan Laporan (STPL) atau Laporan Polisi (LP)
4. Jelaskan kronologi kejadian dengan detail
5. Minta nomor laporan untuk follow-up

Kapan harus lapor polisi:

- Sudah ada ancaman atau intimidasi serius
- Data pribadi sudah disebarkan ke banyak orang
- Uang sudah hilang karena penipuan
- Ada upaya pemerasan
- Teror sudah sampai ke rumah atau tempat kerja[^13]

Pasal yang bisa digunakan:

- UU ITE Pasal 27 (pencemaran nama baik)
- UU ITE Pasal 32 (penyebaran data pribadi tanpa izin)
- KUHP Pasal 378 (penipuan)
- KUHP Pasal 368 (pemerasan)

💡 Tips Penting Saat Melaporkan

DO (Yang Harus Dilakukan):

- ✅ Simpan semua bukti asli, jangan dihapus
- ✅ Buat timeline atau kronologi kejadian
- ✅ Catat semua nomor telepon atau akun yang mengganggu
- ✅ Lapor sesegera mungkin setelah kejadian
- ✅ Laporkan ke beberapa lembaga sekaligus jika perlu

DON'T (Yang Jangan Dilakukan):

- ❌ Jangan menghapus bukti sebelum melapor
- ❌ Jangan takut atau malu untuk melapor
- ❌ Jangan bayar uang tebusan atau ancaman
- ❌ Jangan membuat laporan palsu

📱 SIMPAN KONTAK INI DI HP ANDA

🆘 KONTAK DARURAT KEJAHATAN DIGITAL

📞 OJK
WA: 081-157-157-157
Web: sipasti.ojk.go.id

📞 KOMINFO
WA: 081-1922-4545
Web: aduankonten.id

📞 POLISI
Web: patrolisiber.id
Darurat: 110

📞 SATGAS WASPADA INVESTASI
Web: waspadainvestasi.ojk.go.id
Telp: 157

💡 Foto halaman ini dan simpan di galeri HP!

Ingat: Melaporkan kejahatan digital adalah hak dan tanggung jawab kita sebagai warga negara. Dengan melapor, kita tidak hanya membantu diri sendiri, tapi juga mencegah orang lain menjadi korban. Jangan diam, laporkan!

Daftar Istilah (Glosarium)

Buku ini menggunakan beberapa istilah teknis yang mungkin belum Anda pahami sebelumnya. Berikut adalah penjelasan singkat dan mudah dipahami untuk istilah-istilah penting dalam keamanan digital dan pinjaman online.

📖 GLOSARIUM ISTILAH KEAMANAN DIGITAL

Istilah	Penjelasan Sederhana	Contoh Penggunaan
Phishing	Cara penjahat memancing kita untuk memberikan informasi pribadi dengan berpura-pura menjadi pihak yang terpercaya. Berasal dari kata "fishing" yang artinya memancing	Penipu mengirim pesan WhatsApp berpura-pura dari bank dan meminta kita mengklik link untuk "update data"
OTP (One Time Password)	Kode rahasia yang dikirim lewat SMS atau aplikasi, hanya berlaku satu kali dan dalam waktu singkat (biasanya 3-5 menit) . Berfungsi seperti kunci untuk membuktikan bahwa benar kita yang melakukan transaksi	Saat transfer uang lewat mobile banking, kita menerima SMS berisi kode 6 angka yang harus dimasukkan
2FA (Two-Factor Authentication)	Lapisan keamanan ganda yang meminta dua cara berbeda untuk membuktikan identitas kita. Biasanya kombinasi password plus kode OTP atau sidik jari	Saat login email dari HP baru, selain password kita juga diminta memasukkan kode yang dikirim ke nomor HP kita
Doxing	Tindakan menyebarkan informasi pribadi seseorang ke publik tanpa izin dengan tujuan mempermalukan atau mengancam. Sering dilakukan oleh pinjol ilegal untuk menekan korban agar bayar utang	Pinjol ilegal menyebarkan foto KTP dan nomor HP kita ke semua kontak di HP kita dengan pesan "Ini orang yang tidak bayar utang"

Istilah	Penjelasan Sederhana	Contoh Penggunaan
Tenor	Jangka waktu atau periode pinjaman yang harus dilunasi, dihitung dalam bulan atau hari	Pinjaman dengan tenor 12 bulan artinya harus dilunasi dalam waktu 1 tahun
Plafon	Batas maksimal jumlah uang yang bisa dipinjam dari pinjol atau bank	Kalau plafon pinjaman Anda Rp 5 juta, artinya paling banyak bisa pinjam Rp 5 juta, tidak bisa lebih
APK (Android Package)	File untuk memasang aplikasi di HP Android. Biasanya diunduh dari Google Play Store, tapi penipu sering kirim file APK palsu lewat WhatsApp	File bernama "Undangan.apk" atau "BonusPulsa.apk" yang dikirim lewat WhatsApp adalah file berbahaya, jangan dipasang!
Debt Collector (DC)	Penagih utang yang ditugaskan untuk menagih utang yang belum dibayar. DC yang legal harus sopan dan tidak boleh mengancam	Petugas yang menelpon atau datang ke rumah untuk menagih cicilan motor atau pinjaman
Malware	Singkatan dari "malicious software", yaitu program jahat yang bisa merusak atau mencuri data di HP atau komputer kita	Aplikasi pinjol ilegal sering menyisipkan malware untuk mencuri kontak dan foto di HP
Data Breach	Kebocoran data pribadi akibat peretasan atau pelanggaran keamanan. Data yang bocor bisa dijual di dark web atau dipakai untuk kejahatan	Ribuan data nasabah bank bocor dan dijual di internet gelap
Enkripsi	Proses mengubah data menjadi kode rahasia agar tidak bisa dibaca oleh orang yang tidak berhak	Pesan WhatsApp kita dienkripsi sehingga hanya kita dan penerima yang bisa membaca

Istilah	Penjelasan Sederhana	Contoh Penggunaan
Firewall	Sistem keamanan yang memantau dan mengontrol lalu lintas data di jaringan untuk melindungi dari serangan	Seperti satpam yang menjaga pintu masuk gedung, firewall menjaga pintu masuk komputer atau jaringan

📖 GLOSARIUM ISTILAH PINJAMAN ONLINE

Istilah	Penjelasan Sederhana	Contoh Penggunaan
Pinjol	Singkatan dari "pinjaman online", yaitu pinjaman uang yang prosesnya lewat aplikasi atau internet	Meminjam uang lewat aplikasi di HP
Fintech	Singkatan dari "financial technology", yaitu teknologi yang digunakan untuk layanan keuangan seperti pinjaman, transfer, atau investasi	Pinjol, e-wallet, dan mobile banking adalah contoh fintech
P2P Lending	Peer-to-Peer Lending, yaitu sistem pinjam meminjam uang yang mempertemukan pemberi pinjaman dan peminjam secara langsung lewat platform online	Platform yang menghubungkan orang yang punya uang dengan orang yang butuh pinjaman
Bunga	Biaya tambahan yang harus dibayar di atas pokok pinjaman, dihitung dalam persentase	Pinjam Rp 1 juta dengan bunga 10% artinya harus bayar Rp 1,1 juta
Denda	Biaya tambahan yang dikenakan kalau kita telat membayar cicilan	Telat bayar 1 hari kena denda Rp 50 ribu
OJK (Otoritas Jasa Keuangan)	Lembaga pemerintah yang mengawasi semua layanan keuangan di Indonesia, termasuk pinjol	Semua pinjol legal wajib terdaftar dan diawasi oleh OJK

Istilah	Penjelasan Sederhana	Contoh Penggunaan
Cicilan	Pembayaran utang yang dibagi-bagi menjadi beberapa kali dalam periode tertentu	Pinjam Rp 6 juta dicicil 6 bulan, artinya bayar Rp 1 juta per bulan (belum termasuk bunga)
Kontak Darurat	Nomor telepon keluarga atau teman yang kita cantumkan saat mengajukan pinjaman, untuk dihubungi kalau kita tidak bisa dihubungi	Nomor HP istri, orang tua, atau sahabat yang kita masukkan saat daftar pinjol
Gali Lubang Tutup Lubang	Istilah untuk kebiasaan meminjam uang baru untuk membayar utang lama, sehingga utang makin menumpuk dan tidak pernah selesai	Pinjam di pinjol B untuk bayar utang di pinjol A, lalu pinjam di pinjol C untuk bayar utang di pinjol B

💡 Tips Menggunakan Glosarium Ini

- **Tandai atau highlight** istilah yang sering Anda temui agar mudah mencarinya kembali
- **Catat di HP** istilah-istilah penting yang berkaitan dengan keamanan seperti Phishing, OTP, dan 2FA
- **Bagikan ke keluarga** terutama orang tua atau anggota keluarga yang kurang paham teknologi
- **Simpan halaman ini** sebagai referensi cepat saat menemukan istilah yang tidak dipahami

Ingat: Memahami istilah-istilah ini adalah langkah pertama untuk melindungi diri dari kejahatan digital. Jangan malu untuk bertanya atau membuka glosarium ini setiap kali menemukan istilah yang membingungkan!

Daftar Pustaka (Bibliography)

Berikut adalah daftar referensi yang digunakan sebagai dasar penulisan buku "Sadar Digital: Panduan Praktis Menjaga Data & Melawan Pinjol Ilegal". Referensi disusun berdasarkan kategori untuk memudahkan penelusuran.

A. PERATURAN PERUNDANG-UNDANGAN

1. Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek)
2. Kitab Undang-Undang Hukum Pidana (KUHP)
3. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
4. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)
5. Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan
6. Peraturan Otoritas Jasa Keuangan (POJK) tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi
7. Surat Edaran Otoritas Jasa Keuangan Nomor 19 Tahun 2023 tentang Penagihan Pinjaman Online

B. SUMBER PEMERINTAH DAN LEMBAGA RESMI

Otoritas Jasa Keuangan (OJK)

1. FAQ Fintech Lending. Otoritas Jasa Keuangan. Diakses dari https://ojk.go.id/id/kanal/iknb/data-dan-statistik/direktori/fintech/
2. "Infografis OJK Bersama Kementerian atau Lembaga Terkait Berkomitmen Memberantas Pinjol Ilegal". OJK. 14 Oktober 2021.
3. "Pinjaman Online (Pinjol)". Pasar Modal Indonesia - OJK. Diakses dari https://pasarmodal.ojk.go.id/

Kementerian Komunikasi dan Digital 4. "Laporkan Hoaks ke AduanKonten.id Kemenkominfo, Begini Caranya". Kementerian Komunikasi dan Digital. Diakses dari https://www.komdigi.go.id/ 5. "Laporkan Judi Online". Direktorat Jenderal Penyelenggaraan Pos dan Informatika, Kementerian Komunikasi dan Digital. 24 Juli 2023. 6. "Apresiasi Laporan Masyarakat Komdigi Tangani 1,3 Juta Konten Pornografi dan Judi Online". Siaran Pers Kementerian Komunikasi dan Digital. 2025.

Kepolisian Republik Indonesia 7. Portal Patroli Siber (patrolisiber.id). Kepolisian Republik Indonesia.

Satuan Tugas Waspada Investasi 8. Portal Waspada Investasi (waspadainvestasi.ojk.go.id). Satuan Tugas Waspada Investasi OJK.

C. ARTIKEL ILMIAH DAN JURNAL

1. "Perlindungan Hukum Terhadap Konsumen Pinjaman Online Ilegal di Indonesia". Jurnal Kerta Desa, Universitas Udayana.
2. "Analisis Hukum Terhadap Pinjaman Online Ilegal Perspektif Hukum Perdata Dan Hukum Islam". Jurnal Law Grading, 2022.
3. "Penerapan Hukum Pidana dalam Penanganan Kasus Pinjol Ilegal". Info Singkat DPR RI, Vol. XIII No. 17, September 2021.
4. "Keseimbangan Antara Hak Subjek Data Pribadi dan Kepentingan Publik". Info Singkat DPR RI, Vol. XIV No. 19, Oktober 2022.

D. BUKU DAN PANDUAN

1. "Buku Saku Pinjol". Lembaga Bantuan Hukum Jakarta, 2020.
2. "Buku Digital Safety". Yayasan Kakak Pintar Indonesia (YKP Indonesia), 2023.
3. "Panduan Keamanan Digital Pembuat Konten". Aliansi Jurnalis Independen (AJI), 2025.
4. "Buku Saku Sekolah Desa". Fakultas Ekonomi dan Bisnis Islam, Universitas Metro Lampung, 2023.

E. ARTIKEL ONLINE DAN PUBLIKASI MEDIA

Hukumonline

1. "UU PDP: Landasan Hukum Pelindungan Data Pribadi". Hukumonline, 18 Oktober 2022.
2. "Contoh Data Pribadi Umum dan Spesifik dalam UU PDP". Hukumonline.
3. "Jerat Hukum Pinjol Ilegal yang Sebar Data Pribadi". Hukumonline, 8 Desember 2022.
4. "Pinjol Ilegal Tak Usah Dibayar, Benarkah?". Hukumonline, 20 April 2025.
5. "Terlilit Utang Pinjol Ilegal, Ini Cara Melaporkannya". Hukumonline, 12 November 2024.

6. "Langkah Hukum Jika Dijadikan Emergency Contact Pinjol Secara Sepihak". Hukumonline, 12 Februari 2024.
7. "Tips Terhindar dari Pencurian Data Pribadi oleh Pinjol". Hukumonline, 2022.

Detik.com 8. "Apa Saja yang Termasuk Data Pribadi? Simak Jenis-jenisnya Menurut UU". Detik News, 29 Agustus 2024. 9. "Pinjol Sering Telepon Kontak Darurat, Ini Cara Menghentikannya". Detik Finance, 2 Juli 2025. 10. "Sudah Lunasi Pinjol tapi Tetap Ditagih dan Diteror, Saya Harus Bagaimana?". Detik News, 13 Maret 2024.

CNBC Indonesia 11. "Undangan Kawinan di WhatsApp Bisa Bobol Rekening, Waspada!". CNBC Indonesia, 28 Januari 2023. 12. "Nomor HP Jadi Kontak Darurat Pinjol Bikin Pusing, Segera Lakukan Ini". CNBC Indonesia, 11 Juli 2025. 13. "Cara Mengatasi Debt Collector Pinjol yang Datang ke Rumah". CNBC Indonesia, 4 Oktober 2025.

Kompas dan Media Massa Lainnya 14. "Bahaya Mengintai di Media Sosial 2025: Waspada dan Lindungi Diri". Republika Kaltimtara, 18 Desember 2024. 15. "Jangan Sampai Tertipu! Kenali 7 Ciri Pinjol Ilegal dan Cara Mudah Mengecek Izin Resminya". Suara.com, 30 November 2025. 16. "Akhirnya Data Warga Desa Diakui Tingkat Nasional". Detik News, 14 Oktober 2024.

F. SUMBER LEMBAGA KEUANGAN DAN FINTECH

Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI)

1. "Terlanjur Terjerat Pinjol Ilegal, Apa yang Bisa Dilakukan?". AFPI, 2020.
2. "Cara Pinjol Ilegal Mendapatkan Data Diri Calon 'Korban'". AFPI, 2013.
3. "Jika Mengalami Penagihan Pinjaman Online Seperti Ini, Segera Laporkan". AFPI.
4. "Yuk, Pahami Aturan OJK tentang Bisnis P2P Lending". AFPI, 2015.
5. "Begini Cara Meminjam Dana di Pinjaman Online Terpercaya dengan Bijak". AFPI.

Lembaga Perbankan 6. "5 Tips Dalam Menjaga Kemanan Data Pribadi di Era Digital". Asosiasi Asuransi Jiwa Indonesia (AAJI). 7. "Waspada Bahaya Pinjol Ilegal, Ini Tips Menghindarinya". CIMB Niaga, 25 November 2025. 8. "Pinjaman Online: Tips Agar Pengajuan Cepat Disetujui". CIMB Niaga, 25 November 2025. 9. "9 Ciri-ciri Pinjaman Online Legal, Manfaat, Cara Ceknya". CIMB Niaga, 25 November 2025. 10. "6 Ciri-Ciri Pinjol Ilegal, Risiko, & Cara Menghindarinya". Pegadaian, 4 Juni 2025.

G. ARTIKEL EDUKASI KEAMANAN DIGITAL

1. "Data Pribadi adalah Aset Berharga: Lindungi Dirimu dari Ancaman Siber". Universitas Muhammadiyah Malang, 12 Januari 2025.
2. "Simak 7 Alasan Pentingnya Menjaga Keamanan Data Pribadi". Privy, 25 Februari 2024.
3. "Pentingnya Lindungi Data Pribadi Cegah Eksploitasi Online di Ruang Digital". Kominfo Kota Pekalongan, 14 Oktober 2024.
4. "Bahayanya Jika Data Pribadi Bocor, Ini Kerugiannya!". Bina Digital, 8 September 2024.
5. "Apa Itu Phishing: Definisi, Cara Kerja, Ciri, dan Cara Menghindarinya". Vida, 22 Juni 2025.
6. "Phishing: Pengertian, Jenis, dan Cara Menghindari Phising". Telkom University Surabaya, 13 Maret 2024.
7. "Waspada Modus Penipuan Undangan Pernikahan Via WhatsApp". Polres Jogja, 2023.
8. "Waspada Modus Penipuan File APK: Berkedok Tukang Paket, Undangan Pernikahan sampai Tagihan PLN". Kabupaten Sarolangun, 1 Agustus 2023.
9. "5 Modus Penipuan Terbaru Lewat Whatsapp". Easycash, 8 Juni 2025.

H. ARTIKEL TENTANG SOCIAL ENGINEERING DAN KEAMANAN PERBANKAN

1. "Kenali 4 Modus Social Engineering". Bank BRI.
2. "4 Modus Kejahatan 'Social Engineering' dan Tanggung Jawab Perbankan". Hukumonline, 2022.
3. "Modus Penipuan Social Engineering Mengintai Siapa Saja, Waspada!". Bank Jago, 12 Maret 2025.
4. "BSI Ingatkan Nasabah Waspada Penipuan Bermodus Social Engineering". Bank Syariah Indonesia, 7 April 2025.
5. "Social Engineering: Definisi, Jenis Serangan, dan Cara Mencegah". Bank Syariah Indonesia, 15 Agustus 2023.
6. "Waspada Modus Penipuan Share Screen di WhatsApp". Bank BNI, 23 November 2025.

I. SUMBER LAIN-LAIN

1. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). "Profil Pengguna Internet Indonesia 2024".
2. Direktorat Jenderal Pajak. "Fintech Peer-to-Peer (P2P) Lending dan Potensi Pemajakannya". 17 November 2019.
3. Gerbang Perlindungan Data Pribadi Indonesia. "Hak Subjek Data Pribadi". 7 September 2024.
4. "Warga Digital". Wikipedia Indonesia, 12 Juli 2023.
5. "Warga Digital dan Kewarganegaraan Digital". Binus University, 26 Februari 2023.
6. "Data Pribadi: Definisi, Jenis, dan Cara Melindunginya". Vida, 23 Juni 2024.
7. "Checklist Keamanan Siber untuk Individu: Langkah Sederhana Perlindungan Maksimal". DTrust, 20 April 2025.
8. "5 Keamanan Digital yang Wajib Dipahami agar Data Pribadi Tetap Terlindungi di 2025". Seva, 16 September 2025.
9. "Tips dan Trik Menjaga Keamanan Media Sosial Anda". Diskominfo Mukomuko, 19 Agustus 2024.
10. "Jangan Sampai Kena! Ini 8 Ciri Pinjol Ilegal, Bahaya Teror WA dan Cara Cek Legalitas di OJK". Banjoo, 16 November 2025.

J. KONTAK DAN LAYANAN PENGADUAN

1. Otoritas Jasa Keuangan (OJK)
    - Telepon: 157
    - WhatsApp: 081-157-157-157
    - Website: sipasti.ojk.go.id
    - Email: konsumen@ojk.go.id
2. Kementerian Komunikasi dan Digital
    - Website: aduankonten.id
    - WhatsApp: 081-1922-4545
    - Email: aduankonten@komdigi.go.id
3. Kepolisian Republik Indonesia
    - Website: patrolisiber.id
    - Telepon Darurat: 110
4. Satuan Tugas Waspada Investasi
    - Website: waspadainvestasi.ojk.go.id

- Email: waspadainvestasi@ojk.go.id

Catatan: Semua sumber telah diakses dan diverifikasi keakuratannya pada periode Oktober - Desember 2025. Beberapa referensi merupakan sumber publik yang dapat diakses secara bebas untuk kepentingan edukasi masyarakat.

BIOGRAFI PENULIS

Cekli Setya Pratiwi, SH., LL.M., M.CL., Ph.D.

Cekli Setya Pratiwi adalah dosen dan ahli hukum di Fakultas Hukum Universitas Muhammadiyah Malang sejak tahun 2000. Beliau menyelesaikan pendidikan di empat negara: Sarjana Hukum dari Universitas Brawijaya (1998), Master of Laws dari Utrecht University, Belanda (2006), Master of Comparative Law dari Brigham Young University, Amerika Serikat (2019), dan Doktor dari Mahidol University, Thailand (2024).

Keahlian beliau meliputi Hak Asasi Manusia, Hukum Tata Negara, Hukum Internasional, dan Hukum Syariah. Dr. Cekli adalah penulis produktif dengan karya yang dipublikasikan secara internasional, termasuk buku "Sharia and Human Rights: A Course Book" (2022) dan "Hukum Internasional Publik: Konsep, Norma dan Studi Kasus" (2024). Karya beliau meraih penghargaan Penulis Terbaik Nasional Peringkat Kedua dari Perpustakaan Nasional Indonesia pada Oktober 2024.

Beliau aktif sebagai peneliti untuk Komnas HAM dan konsultan kebijakan hukum, serta menjabat sebagai Sekretaris Jenderal SEPAHAM Indonesia (Konsorsium Dosen HAM Indonesia) periode 2022-2027. Dr. Cekli sering menjadi pembicara di konferensi internasional, termasuk di Universitas Oxford, dan berdedikasi dalam memajukan pemahaman tentang hukum dan hak asasi manusia.

Prof. Dr. Sidik Sunaryo, SH., M.Si., M.Hum.

Prof. Sidik Sunaryo adalah Guru Besar Ilmu Hukum lulusan Fakultas Hukum Universitas Muhammadiyah Malang (1990), dengan gelar Magister Sosiologi (1994), Magister Hukum (2012), dan Doktor Ilmu Hukum dari Universitas Brawijaya (2016).

Keahlian beliau meliputi Sistem Peradilan, Sosiologi Hukum, Metode Penelitian, dan Kriminologi. Sejak 2004, Prof. Sidik konsisten meneliti putusan hakim di Indonesia dan negara lain, dengan fokus pada hukum pidana, korupsi, dan reformasi peradilan. Penelitian beliau menghasilkan banyak karya penting tentang Sistem Peradilan Korupsi, Good Governance, dan Perbandingan Putusan Hakim Indonesia-Amerika.

Prof. Sidik adalah penulis produktif dengan banyak artikel di jurnal nasional dan internasional bereputasi, serta telah menulis beberapa buku referensi. Beliau aktif sebagai pembicara di seminar internasional, termasuk di Brigham Young University, Amerika Serikat. Melalui dedikasi dan kontribusinya, Prof. Sidik terus mendorong reformasi peradilan untuk mewujudkan keadilan bagi masyarakat Indonesia.